Witness Seminar
“Between a Rock and a Hard Place?: Can Governments Respond to the COVID-19 Pandemic and Still Respect Personal Privacy?”

Tuesday, May 5 3:30-9:45pm UTC (8:30-2:45pm Pacific Time)
Preface

The objective of this Witness Webinar was to bring together experts on ethical, legal, and social implications of public health technologies to 1) explore the challenges, risks, and benefits of deploying novel technologies in the response to COVID-19, 2) open a dialogue with public health officials and the public about the challenges, risks and benefits, and 3) use the exploration and dialogue to write a public policy paper that lays out the challenges, risks and benefits, and a framework that can be used in public policy decision-making and privacy-preserving technology design.

The Witness Webinar drew upon the Witness Seminar methodology, which was developed in the 1990s by The History of Twentieth Century Medicine Group of the Wellcome Trust. It is interesting to note that the first such seminar explored the subject of monoclonal antibodies. Witness Seminars began as a novel approach to oral history and evolved into a gathering of numerous participants who are recorded simultaneously and able to interact with each other and with the seminar convenor. The Witness Seminars produce group discussions on topics of special interest and make collective oral history materials (e.g., transcribed proceedings) available for widespread use.

Given the social distancing restrictions in place to prevent the spread of COVID-19 at the time of the event, it was necessary to adapt the Witness Seminar methodology to enable exploration and online participation and engagement. The seminar, which was renamed a “Witness Webinar”, took place using the online Webinar platform Zoom over one day, May 5, 2020. The agenda appears as Appendix A.

For this Witness Webinar, the organizers (the “Working Group”) sought to identify as broad a range of “Lead Witnesses” representing as many perspectives as possible in order to explore the motivating question thoroughly. Lead witnesses, invited according to a snowball sampling technique, included individuals from academia, the public sector, the private sector and non-governmental organizations with backgrounds in public health policy and research, biomedical research, ethics, law, technology, communications, privacy and data protection, civil liberties, primary health care, art curation, and entrepreneurship from Canada, the United States, Australia, the UK, Ireland, Switzerland, and Japan. A full list of Lead Witnesses and their backgrounds appears as Appendix B. The Honourable Joyce Murray, Canada’s Federal Minister for Digital Government, opened the proceedings.

Style of Interaction: During the Witness Webinar, each Lead Witness was invited to present a five-minute statement representing their views on the motivating question.

---


2 The methodology was changed to the extent necessarily to allow for online versus in person interaction, and was reviewed and approved by UBC’s Behavioural Research Ethics Board (Ethics Certificate Number H20-01411).
Most participants had prepared scripts, but they did not use slides or other visual material. Each statement was followed by a 10 minute question and answer session during which Lead Witnesses first responded to questions or comments from other Lead Witnesses posted in the Zoom chat area followed by questions or comments from anonymous webinar participants, who posted their questions and comments in the Zoom “Q&A” area. Questions and comments from participants could be “up-voted” by other participants to increase the likelihood of a response though it was left to the discretion of each Lead Witnesses to respond.

Interactions were informal in nature and as spontaneous as the online platform allowed. We used the Witness Webinar format as a form of open peer-review, with all remarks and opinions immediately subject to rejoinder, agreement, or dispute from others.

**Publication of the Witness Seminar:** The complete proceedings were recorded and transcribed using transcription software. All participants took responsibility for their own remarks, the copyright of which was assigned to UBC to allow for publication. Following production of the transcription, a copy of the unedited transcript was sent to all participants for them to amend their own contributions. Minor corrections and comments were incorporated into the master text, and, in some cases, participants also added section headings to further contextualize their remarks. Additional contributions, such as citations to external sources, were added as footnotes.
Acknowledgements

I would like to thank the Peter Wall Institute of Advanced Studies (PWIAS) for funding the Witness Webinar, and for technical and administrative support. In particular, I would like to thank Bernadette Mah, PWIAS Program Manager, and Aurora Tejeida, Communications Coordinator, for their assistance. I would also like to thank Blockchain@UBC, in particular, Michelle Ho, Program Coordinator, for additional administrative support, and Anisha Dhillon, graduate student at UBC’s School of Information, for assistance with coordination of the Witness Webinar, preparation of the proceedings, and compilation of background information related to COVID-19 technology use cases.

I would be remiss if I did not express my sincere gratitude to The Honourable Joyce Murray for her opening remarks and to all the Lead Witnesses who took time to participate and present thoughtful remarks on the challenges facing society at the intersection of COVID-19, technology and data privacy during this critical time for people around the world.

Finally, I would also like to express my gratitude to the members of the Working Group, Charles Dupras, Holly Longstaff, Samantha Pollard, Jennifer Pougnet, and Chandana Unnithan for their assistance with identification of the experts who participated as Lead Witnesses and for their additional editorial contributions to the proceedings and accompanying policy brief.

Victoria Lemieux
Working Group, Chair
May 30, 2020
PREFACE
ACKNOWLEDGEMENTS
VICTORIA LEMIEUX, OPENING REMARKS AND WELCOME
HON. JOYCE MURRAY, FEDERAL MINISTER FOR DIGITAL GOVERNMENT, OPENING REMARKS
ANN CAVOUKIAN
LILI LIU
JENNIFER POUGNET
ROBIN RENWICK
CHANDANA UNNITHAN
CIARA STAUNTON
HOLLY LONGSTAFF
YANN JOLY
CHARLES ALESSI
NADIA DIAKUN
MICHAEL MCDONALD
ROBERT FRASER
MICHAEL CHOLOD
JESSE MCKEE
STEVE MAGENNIS
PAOLA ARDILES
Victoria Lemieux, Opening Remarks and Welcome

Vicki Lemieux [00:00:05] So good morning, everyone who's just joined. I'd like to welcome you.

Vicki Lemieux [00:00:12] It's very exciting to be here, too. To conduct this witness seminar, which we've called between a rock and a hard place. Can governments respond to the COVID-19 pandemic and still respect personal privacy? We, I must say, we've been overwhelmed by the level of interest in this seminar. It's clearly a topic that is on everyone's minds, especially at the moment where we see governments and different jurisdictions and groups organizing to deliver technologies that can help fight the pandemic and get us back into some kind of semblance of a normal existence. So, it's an extremely timely topic, but we, we face many challenges with making policy about how we roll out these technologies and indeed designing and developing this tech, these technologies at the speed of a pandemic. It doesn't give us a lot of room to pause for thought. And so what this witness seminar really is all about is doing that: trying to create a space where we can bring together global experts - and I thank all of our lead witnesses for taking the time to be here - to pause for thought in what we're doing in rolling out these technologies and how we can properly balance the need for public health and safety and the right to privacy.

Vicki Lemieux [00:02:02] We will meet until 3:00 p.m. So it's a bit of as one of our lead witnesses said, a bit of an intellectual marathon. I'm not expecting that everyone will be glued to Zoom the entire time. I fully expect that you'll need to maybe come and go. We do have an official break for about 15 minutes in the middle of all of this. But obviously, if you need to, to break as we go, I'll just remind everyone that we will be recording this so that we may transcribe it and make the proceedings public. That's part of the process of witness seminars.

Vicki Lemieux [00:02:38] I would be remiss if I didn't mention the Peter Wall Institute for Advanced Studies here at the University of British Columbia, who have provided the financial support to make this possible. It takes a big team to put something like this together, especially on short notice. The financial support of Peter Wall has been very instrumental in that. And I'd like to acknowledge Michelle Ho in particular and my team here at Blockchain@UBC in general for their excellent work in helping to organize this witness seminar. So a bit of a history about witness seminars. They were developed in the 1990s by the history of 20th Century Medicine Group of the Wellcome Trust to enable participants to come together. They're usually recorded simultaneously, as we're doing today, and allow participants to interact with each other. Typically participants would come together physically, but of course these are novel times. And so we are
doing this virtually, coming together virtually to discuss topics of special interest, to make a collective oral history for widespread use that’s transcribed and the proceedings are made public. So recognizing that COVID-19 is a phenomenon of historic importance for us globally, and it's raising many, many challenging issues, we felt it appropriate to conduct this witness seminar as a way to capture where we are. And as I say, pause for collective thought on the technologies that we're using to assist us.

Vicki Lemieux [00:04:25] The other purpose is really to engage with our lead witnesses to try and create a panorama of the various policy options, the approaches that are being taken. The issues that surface as well as we roll out new technologies to address the pandemic, because policymakers, governments worldwide are being faced with a challenge. And in the digital world, obviously, technology has got to be one of the solutions. But when you're trying to make policy at the speed of a pandemic, you really don't have time to think things through. So we can help.

Vicki Lemieux [00:05:10] We felt by collecting together, curating a range of issues and policy options, approaches, considerations that policymakers then have at their disposal to address this issue in a way that they would necessarily not have time to curate or collect themselves from a diverse range of voices and to do it in in a manner where we are, as I say, pausing for reflection and thought; we're not in the heat of the moment.

Vicki Lemieux [00:05:50] So we felt this would be very helpful because policymakers are having to make some hard choices at the moment and they're having to make those choices quickly.

Vicki Lemieux [00:06:01] And so to ensure that they're as well informed as possible, that we ourselves, as we design new technologies, as we're engaged in actively trying to address and fight the pandemic, and determine how help individuals around the world, as you know, as we're motivated to do that, we ourselves would benefit from this kind of a conversation. My own interest in this is that I have been involved as the co-lead of Blockchain@UBC, which is the University of British Columbia's Research and Education Center cluster focused on blockchain and distributed ledger technology, we are a multi-disciplinary research group that started in 2017 to look at blockchain technology and related technologies of decentralized trust and how to design them, but also the implications for society of these technologies. So in that context, I've been researching the use of blockchain technology for privacy, preserving health data management and sharing. So this is a topic of keen interest to me. And as I mentioned to the lead witnesses earlier, I really am interested in learning from all of you. So I thank you all for being here and agreeing to do this.
We have an exciting day ahead of us, but we should just remind ourselves of how the proceedings will be conducted. So the idea is that we will have each of our lead witnesses who will give a five minute presentation after the opening of the proceedings. Each of those lead witnesses will, after following their five minute presentation, during which they'll present their own unique perspective on the question, the central focus of our witness seminar. We will turn to the Zoom chat, where other lead witnesses will be posting questions and comments and they'll take five minutes to address one or two of those questions or comments. We're on a very tight schedule, so we won't be able to address every single question or every single comment, but these will be captured as part of the proceedings. The lead witnesses will then turn to the question answer section of the Zoom, where participants will be able to post questions. And I'll just remind participants that you should be posting your questions anonymously to protect your own privacy. So we've tried to set this up and configure the Zoom so that it would be for those who are not here as lead witnesses, as as public scholars or other individuals who are willing to put their views forward publicly that your own privacy would be protected. So make sure your camera's off. You've logged in under a pseudonym and that you post your questions anonymously. But you when you see a question that you would like to have addressed by a lead witness, you can upvote that question and the lead witness will address the questions that likely get to the top. It is entirely the lead witnesses’ choice as to whether they feel able to address the particular questions. Again, participants shouldn't expect that every question, even the ones that reach the top, would be addressed. It really is up to the lead witnesses as to whether they feel they wish to address that particular question at that particular time. But we will be capturing all of the questions as part of the proceedings.

The other important thing to remember is that this is again, a space of pausing for thought and we want to be reasoned and reflective in our approach. So I would just remind everyone that the questions and the comments in the chat and in the question and answer section should be thoughtful and reflective and should be asked in a spirit of scholarly inquiry rather than trying to politicize or engage in political commentary, because we are in a moment of crisis and at a pressing moment. And there are certainly issues of pressing concern to us. But we do want to keep this as a space of more reflective engagement. So with that, I think we're ready to move on. I don't know if we have Minister Murray, yes I see Minister Murray there. So I would like to we should say that we will not be doing long introductions of our lead witnesses. But I would like to spend a moment to introduce you to Minister Joyce Murray, who is Canada's Federal Minister for Digital Government. And we're delighted that she is joining us here today. She's taking a few minutes before she has to join virtual parliament. So everything is online and virtual these days, too, to share with us
her opening remarks and reflections to get us started. So thank you very much, Minister Murray, for joining us this morning. It's a pleasure to have you here. And I'll just turn it right over to you.

Hon. Joyce Murray, Federal Minister for Digital Government, Opening Remarks

Joyce Murray [00:11:58] Thanks Vicki. I'm really pleased to have been invited. I want to acknowledge I'm here on the traditional unceded territories of the Musqueam, Salish and Tsleil-Waututh First Nations joining you in this really important conversation. And thank you for putting it together. Your call for a collaborative approach is so much in the spirit of what we've been seeing across the country and around the world - a new level of collaboration and cooperation as we realize we're all in this together. So bringing brains and ideas together today is super important. And I want to help. I also want to wish you and your families well. J'espère que vous et vos familles êtes en santé et en sécurité.

Also, of course, thank you to the University of British Columbia for organizing this event and using this great digital tool to make it possible to meet while physically distancing, which perhaps won't be forever. But it's important right now. And the conversation around privacy. And where are we going to go, post-COVID is so important. Your work to facilitate this important conversation and promote different perspectives on privacy is more critical now than ever.

Joyce Murray [00:13:29] In a way, it's pretty much a cliché, but I think that a crisis is a very important time to think about the opportunities to do things differently and better.

Joyce Murray [00:13:51] It's no secret that we find ourselves in a time that is very challenging.


Joyce Murray [00:14:12] We have been very involved as digital government, as you can imagine. The government has had a massive response quickly rolling out financial supports to make sure that Canadians can pay their bills and businesses and employers can and protect jobs and can pick up the pieces and hit the ground running after this emergency. This crisis has really engaged the digital government in a way I couldn't have imagined before. If you can imagine having the entire public service almost overnight, working from home. Think of the infrastructure, the tools, the bandwidth, the
technology that was needed for that. And I want to give a shout out to all of the teams at Digital Government who responded quickly and effectively to make that happen.

As well, there are millions of Canadians that are being served with new benefits and information. There is an underpinning of digital delivery that has kicked into gear to help make the government as effective as possible. Federal governments are not necessarily known for being agile and fast. And I want to say publicly that I’m extremely impressed by the incredible work the public servants at Shared Services Canada, and the Office of the Chief Information Officer and the Canadian Digital Service – the teams who support me and my mandate - have been doing.

Not only do they support the ongoing operation of the government’s IT infrastructure and systems, but they ramped up its capacity and resilience virtually overnight, and quickly developed new digital tools and solutions.

Joyce Murray [00:16:12] So how have we accomplished this so quickly? I think one thing that stands out is that the risk calculation changed. Governments are always very cautious about doing anything that creates risk. And that’s correct especially when considering the risk of a privacy breach.

Joyce Murray [00:16:39] But I can say that throughout the speed of our government’s response to this pandemic, we have maintained our utter commitment to privacy. But there are other risks, for example, what if we get this wrong? Are we going to give out too much money? Some of these risk calculations have changed because the risk of doing nothing is suddenly elevated in a situation like this.

Joyce Murray [00:16:58] So we are very quickly putting in place a massive set of unprecedented changes. But privacy is something that we have really focused on over the course of this and we'll continue to do so because privacy is so important to the government. And let me tell you why. Because when you think about the public policy around what government's role is, it is to deliver excellent service to Canadians whether we are in crisis or not. It is to ensure we are not wasting taxpayers money and we can still deliver services that Canadians rely on. And most importantly to have the trust of its citizens.

Joyce Murray [00:17:59] That's why privacy concerns are so incredibly important and why it's so important that you're looking at that nexus between government policy, service delivery and the trust that citizens have to have in their government.

Under normal operating circumstances, no organization is immune to IT security
threats. But we all know that these are extraordinary times. A particular challenge for governments around the world is the spread of false information, which is something we’re keenly focused on. To combat misinformation surrounding COVID-19, we have developed a web-based email service that gives subscribers authoritative information about COVID-19, called “Get updates on COVID-19”.

As important as all of these efforts are, however, they will not be successful unless we ensure that the privacy of Canadians is respected.

Joyce Murray [00:19:35] This is especially true with regards to digital contact tracing.

Joyce Murray [00:19:52] We have had conversations with a number of companies working on different models that might be applicable here in Canada. But I want to be very clear that any decision we may or may not take with regard to COVID-19 contract tracing would have to meet Canadians’ high standards for privacy and ethical use of those technologies. As the Prime Minister has said, getting that balance right will be extremely important.

These high standards for privacy are also reinforced by the Privacy Commissioner of Canada, with whom I had the pleasure to meet a few days ago. We have ongoing engagement on many initiatives with privacy impacts, and I value this productive collaboration.

So that's some of what we'd been doing. As we move forward to a period where Canada gets through this pandemic – we need to ask ourselves what did we learn and how have we changed our society for the better? The work that you're doing here today is really important.

Joyce Murray [00:20:24] Collectively, the Herculean Coronavirus digital response and public health response and the public servants and all of society’s efforts have not been without challenges. But I think we can all be proud of what's been done to date and we can take these lessons learned. Seminars like this one are important spaces for discussion and debate about how public policy makers can get the balance right.

Joyce Murray [00:21:46] I really do regret I'm going to miss most of the discussion today on this because I'll be in a new digital innovation, which is virtual parliament - an important way to connect with Canadians during this time So thank you for what you're doing, Vicki. Enjoy your day, merci.
Vicki Lemieux [00:22:05] Yes. Thank you. Merci à vous aussi.

Vicki Lemieux [00:22:09] And we really appreciate the fact that you've taken the time to come in and open the proceedings and share with us the challenges. Amazing difficulties, I'm sure, to turn such a big ship around. The federal government of Canada and do you know, release new programs, even come up with these new programs, make sure that Canadians can access the new program. So I have to say, as a Canadian, I'm very proud of what our government has been able to do, as well as very aware of the challenges that we've faced and the little time that we've really had. I'm sure that you've had as a government minister with your colleagues, you've not had the same time to really think through in the level of detail that you would normally, as you say, assess the risks of all of these policies. So we very much appreciate the huge challenge that our leaders have taken up with a great responsibility. Thank you for taking time to open the proceedings and get us started. And we recognize that you haven't got time to stay for questions.

Vicki Lemieux [00:23:28] And because you've got to get into virtual parliament and of the business of democracy must go on [laughter].

Vicki Lemieux [00:23:37] So thank you for being here.

Joyce Murray [00:23:37] Vicki, If I may and I'm just seeing Ann Cavoukian on my screen here and I wanted to say hello and thank you for all the work you did. Ann and I worked together on a private member's bill project a number of years ago.

Joyce Murray [00:23:55] And I have such respect for you Ann. So it's great to see you here being part of this conversation.

Joyce Murray [00:24:02] And I'm going to sign off now and thanks again for putting this on.

Vicki Lemieux [00:24:08] Thanks very much for joining us, Minister Murray. Thank you. All right. Take care.

Ann Cavoukian

Ann Cavoukian [00:29:22] Let me get to the point in terms of what does a COVID-19 pandemic mean in terms of privacy and our freedom.
It could be devastating, but we're not going to allow that to happen. You see whenever there's a huge problem, in this case, it's a pandemic. In previous cases, it's been acts of terrorism, think of 9/11. What happens are under emergency powers, additional information is captured about citizens. It's theoretically always supposed to be used during the peak of the time frame of the crisis. But what happens is it often lingers afterwards. Tracking and surveillance of people's activities continues after the emergency is over. Think of 9/11, I was privacy commissioner at that time. It was, I think my second term, and it was devastating. Of course, what would happen after 9/11 ended with even more devastating. Surveillance was massive. In the United States, you had the Patriot Act introduced, which was all encompassing. You had the department, Homeland Security created and huge in terms of the surveillance. It could engage on and on. And Canada wasn't oblivious to that.

So my concern here with this pandemic. There will be an end date. It will end. My fear is that the tracking of personal information that they engage in now under emergency powers on your privacy laws, that that tracking could continue well after the crisis is over. So we have to ensure. The following we have to ensure there are a firm sunset clauses end dates. Related to the tracking and surveillance that's taking place under emergency powers. It has to have a firm sunset say June 1st and then you can revisit it to see if it needs to be extended, but it cannot be without a firm end date. And at that time, all of the data collected thus far must be securely deleted. We cannot allow these kind of incidents to rob us of our privacy and our freedom.

Privacy forms the foundation of our freedom. You cannot have a free and democratic society, a solid, a foundation of privacy. And we know this historically. Look at Germany. It's no accident that Germany is the leading privacy and data protection country in the world. It's no accident. That they had to endure last year, the Third Reich and the Stasi, the police and the stifling of all of their freedom and privacy. And when that ended, they said never again, never again will we allow the state to strip us of our privacy and our freedom and do a right. It was wonderful. They stood up to that. I went to many conferences during my three terms as privacy commissioner. Every conference in Germany was started with a reference back to that time. Lest we forget.

So I don't want you to forget the unbelievable value of privacy and freedom. I don't want you to let this serious crisis. Now, there's no question at the end, everything is such that when it's ended and it will end, our freedoms will not be restored and privacy will not be preserved. That's what a lot of people have been saying to me lately, you know, give it up, lady. That ship has sailed, over my dead body it has sailed. You don't give up on privacy and freedom. You see you have to understand my background. I'm Armenian. My grandparents barely escaped the Armenian genocide. They ended up in Egypt. I
was born in Cairo. We came to Canada when I was four years old and in Cairo, it was under British rule. My mother told me everything was wonderful and they had freedom. Until the British called out and Abdel Nasser came in and mid-50's. That was the problem the late 50s. If he changed everything, the government had controlled everything. And my parents couldn't tolerate raising their family. As I said, I was four years old. Under those conditions of no freedom, given what the grandparents had to endure. So they literally left in the dead of the night, coming to Canada, staying in the basement of some dear friends of ours until my father could get his business up and running. It was a terrible ordeal to go from such an amazing life to something where you're living in a basement was functionally no funds and three children who were driving you crazy. So I say all this to tell me how much we value freedom. And what we know happens when you lose freedom and you lose privacy. We cannot allow that to happen here.

Now some good news. Apple Google framework. They've developed an app, an API that is amazing in terms of the strength of its privacy provisions. It is completely privacy protected. The user's ID gone. The geolocation data gone. Any individual who self-report that they're COVID-19 positive will never be identified. It preserves privacy like no other. It uses Bluetooth, which sends out beacon transmissions, which change about every 15 minutes. And even that is encrypted using a. I mean, it's remarkable. So there's hope. Also, two letters were sent out in the last few weeks. One from 300 academics and epidemiologists from all around the world saying unless you strongly preserve privacy, it will not work. This contact tracing, it will fail. Just a few days ago, last week, another group of 170 academics and epidemiologists etc. from all around the world said essentially the same thing. Any attempt to do contract tracing that doesn't preserve privacy. Hundred percent will fail to stop. So I just want to make it clear to you, this cannot be viewed as an either or Zero-Sum proposition. It's not. We have to have public health and privacy. Not one versus the other. It can't be win, lose, lose. We need multiple positive gains making a win win proposition. We can do this. Thank you very much. I think I've exceeded my five minute timeframe.

Vicki Lemieux [00:36:11] That's that's OK. We are a little bit ahead of schedule. And that's a good thing because we wanted to hear from you. Especially since you are opening. You're our lead witness. Opening the session today. And so since you are not able to see the dashboard at all what I thought I would do is just read out questions and comments, and we can have a little bit more of a discussion. Your own personal story is is very, very compelling. And thank you for sharing that, because it reminds us, you know, just what we stand to lose. And we never really think that we will lose that in a you know, in the kind of society that we live in for most of us. But things can change very quickly. And so your personal story is the story of how those things can change. All
those things that we took for granted may just not be there one day. And if we think of how quickly our lives transformed under this pandemic and how, you know, some of us, just as you were when you were younger, are living in the basement without funds, we can certainly appreciate how quickly things can change. So I wanted to just acknowledge that there are some questions here in the Zoom chat. And so there’s a question from our lead witness, Kohei Kurihara, from Japan. So just so you know, there are lead witnesses and participants from all around the world. And Kohei is asking, how can we fight against government privacy surveillance such as data abuse when this pandemic becomes alleviated? Is there any structure or any strategy that you would recommend?

Ann Cavoukian [00:38:07] Thank you. I would urge privacy commissioners all around the world to step up and actively meet with governments and ensure that whatever was collected during the time of the pandemic. First of all, stop in terms of any possible continued data collection and surveillance and that the data be fully erased. If I was commissioner, what I would do, actually I would do it right now, I would meet with Premier Ford, who in Ontario is our premier. I would meet with him and I would say, “I want to ensure that our government is doing the least possible to harm privacy.”

I understand that there are some concerns in terms of tracing people, and I actually hate that term. One of the things I love about the Apple Google framework is they're calling it exposure notifications, so individuals can be notified when they've been exposed to someone who is COVID-19 positive. That's all you need. You don't know their name. You don't need to know where they live. You just need to know you've been exposed so you can go and get tested and take the precautionary measures. So what I would do if, please consult with a privacy commissioner in your jurisdiction, ask them. Are they meeting with the government? No. Don't wait until the pandemic is over. I would plan a series of steps. What will you be doing? What are you doing now to protect privacy during the emergency powers? And what kind of contact tracing are you encouraging for the public? Because that's the next step. And then I would chart out exactly when is a sunset clause, the firm end date to the tracking, is going to take place. And I would be happy to meet with you to revisit that at that time to determine whether it should be continued or not. But we must have permanent sunset clauses. And then once the sunset clause takes place and let's say the pandemic is over, I would meet with them again to ensure that all of the data collected are no longer being collected and are being securely deleted, completely. There should be no government collection and retention of this data during the pandemic emergency situation. These are very important steps for privacy commissioners to take in. I'm sure they'll be taking them, but I urge them to move now. Don't wait. You have to be proactive on this.
Vicki Lemieux [00:40:37] Thank you. Those are some really great strategies that you've outlined. I'd like to drill down into another question that's come up on the chat from Jennifer Pougnet, who is asking, what do you believe needs to happen post COVID to enable more effective response to future crises globally. So this is thinking about maybe the next pandemic. Heaven forbid, for the next crisis of whatever stripe you mentioned the Patriot Act, that was an act of terrorism. We know we can't predict these unpredictable events in some way, but we can predict that they're likely to happen. So how would we best prepare ourselves for that?

Ann Cavoukian [00:41:24] I think it's really important to have a game plan in place in anticipation of hopefully not future pandemics, but future whatever, and the ideal time is at the end of this long one. Everything has been sorted out and the data's been deleted and tracking is stopped and private citizen preserved meet with the government bodies that are working on this or they're probably not working on it. Meet with them. Start with the premier's office and lay out a plan of how would we proceed next time. It's absolutely essential to put something in place in terms of what information do you truly need? That's the whole point of data collection. This is all about control, personal control over the collection and uses of your data. Citizens have a right to know what the government's collecting upon them and how long they're going to be keeping it. And there's something called the primary purpose of the data collection.

Theoretically, the government will only want to collect information to make determinations relating to a future pandemic or a future terrorist attack or whatever. Let's have a solid plan as to what. What do you require? And it will vary depending on the nature of the crisis, of course, somewhat a health related some might be terrorism always so might be something else. But we have to have a solid game plan. It doesn't exist now. That's the problem. And hopefully that can be one of the things that emanates out of this. Again, if I was privacy commissioner, I would meet with the government after we got rid of all the data already collected and set up a game plan, hopefully not anticipating future events or preparing for them in terms of how these should be addressed. It's absolutely critical. And to say something about governments.

When I was privacy commissioner for three terms, there was a different political party in the government in each of those terms. We started with the NDP and then I think with the Conservatives and then the Liberals. And before that party became the government, they were all interested in privacy. They cared deeply about people's privacy, want to preserve, protect, etc. But the minute they became the government, all that changed. Then they wanted to be in control of the data. And this is what concerns me. Governments love having control over data. Well-intentioned, I'm sure, but I don't trust it in the hands because the ability to use it for secondary uses, other uses other than the
primary purpose of the data collection. Staggering. And we'll never know if it's used for secondary uses. Certainly, without our consent.

So we always have to be very, very cautionary position in terms of the privacy. And I pray that I'm wrong and that everything is going to be fine. But trust but verify. You always have to look under the hood to ensure that our privacy laws are strongly followed. That our privacy is strongly protected. And that the need for privacy and the importance hasn't been diminished because of this last pandemic. We can never make it a win lose either or when it comes to privacy. I can assure you it's never privacy that wins over the other interests. Nor am I suggesting it should. But I sure as heck am not going to lose out every time. So I want multiple positive games at the same time, and we have to put that mentality into the government.

Vicki Lemieux [00:44:57] Thank you. I think those again are some really wise words. And I'm glad you mentioned the link between access to information and privacy, because as you pointed out, we need to know what information the government's collecting on us. I'd like to link this to a question that I have for you, which is that when we have public private partnerships where maybe, you know, Apple and Google, as you said, you knew, felt that they were doing a good job of protecting privacy. But we can point to some public private partnerships where the kind of data that is being collected on us and how it's being used is not necessarily subject to access to information legislation nor very transparent. And I wondered about how we can make sure under those circumstances that if there's a sunset clause on data, data collection and data use, that that's actually being implemented post pandemic, that we're actually able to ensure compliance with those restrictions. Do you have any reflections on how we should address that?

Ann Cavoukian [00:46:12] Again, I point to the information and privacy commissioners in every province and federally. When I was Privacy Commissioner, I didn't report to the government, I reported to the legislature. Thank God. Otherwise, I would have been fired on day two because we're investigating the government and their activities. And the legislature fortunately consists of all three political parties. So it's incumbent upon the privacy commissioner to ensure that the proper activities are taking place, that governments are not exceeding their world, especially in public private partnerships. I'm actually less concerned about the private partnership, the private sector entities than the government because it was the private sector. You can make it very clear these are the terms you abide by them or you don't. That's the deal. That's how we form a partnership.
And I can tell you, having worked with Apple over the years. I mean, Apple cares more privacy than most governments. You know, they provide an end to end encryption, which is amazing. They bond James Comey, the attorney general in the United States, when he wanted them to open up the code for somebody's mobile phone Apple that they had gotten. And Apple said we can't we don't have the key. It was issued. They took a very strong position. So and so the Apple Google framework is 100 percent privacy protected more than anything. And in fact, they're giving that framework to public health authorities to develop the contact tracing app. And they basically said to the public health authorities, you must make whatever you're doing accessible for otherwise open source so that we can ensure that all the protections we've embedded in our framework is reflected in your public sector API app that you're developing for this. And there's transparency everywhere in this. You can look at the code. You can look at Apple, Google Frameworks code. It's all open source. So transparency is very, very important. And we need to make it clear that there cannot be a weakening of privacy or transparency because you've got public partner partnerships. It should elevate those two areas, not weaken them. We insist upon it. No.

Vicki Lemieux [00:48:31] OK, great. Now, I'd like to turn to a question that's in the Q&A. And then if there's time, come back to another comment in the chat. So you, I'm sure, would have heard of this concept of self-sovereign identity.

Ann Cavoukian [00:48:31] Yes.

Vicki Lemieux [00:48:31] Yes and so the attendee has asked would sell sovereign identity data collection be encouraged for those facing self-isolation, issuing a credential at the end of their isolation and then revoking the credentials. So maybe they're kind of trying to picture a scenario here, but maybe you could comment on this self-sovereign identity technology and where you maybe see that fitting into things.

Ann Cavoukian [00:49:22] I'm a big fan of self-sovereign identity. Drummond Reed, and I wrote a paper together when I was privacy commissioner and he's leading the charge on this with his company Evernym. I mean, it's it's amazing. And self-sovereign identity basically encapsulates what privacy is, which is personal control, control over your personal information that you should be in charge. Self-sovereign identity, you should be in charge of your identity and your personal information. And it's decentralized. That's what I love about it. It's a decentralized model where your personal information is

---

under your control in a decentralized. It could be in a secure enclave in the cloud. It could be a blockchain venture. There are many ways in which this can take place.

Now, I haven't applied SSI yet in my mind to the COVID-19 crises just because I've been going crazy with COVID-19 and trying to ensure privacy is respected. But we could see how this could work together. Decentralized solutions are amazing. Like I said, I had about a year and a half ago. Tim Berners-Lee went public and he said the creator of the World Wide Web. He went public and he said, I'm devastated what I created and the World Wide Web. It's become a centralized honeypot for data collection by the, you know, the big companies that Facebook, Google, etc. And they can do whatever they want with their information, which is in their centralized database and it's under their control, not yours. You said I'm leaving that and I'm going a decentralized route. He created something called solid. But now there are multiple decentralized channels that are growing, which are returning control of data to individuals and putting it in their own secure enclave. It could be an SSI framework to be somewhere else. So I find this very promising. And it's certainly something we could explore in the context of after a COVID-19.

Vicki Lemieux [00:51:18] Great. Thank you for that. And now, I guess, you know, in a little bit of a kind of reverse scenario or thinking about, you know, not having data, then. So we e pass the sunset clauses, we delete everything.

Vicki Lemieux [00:51:33] So Michael McDonald is asking, but if we do that, excuse me, post-crisis, how will we learn from our successes and mistakes?

Vicki Lemieux [00:51:44] So there needs to be intel room for intelligent research. So he's saying he's advocating for some data preservation because maybe some of that data is data that we can analyze. We live in a world of big data. We learn a lot from our big data. So. What happens if we destroyed it all?

Ann Cavoukian [00:52:04] The only part I'm suggesting we do destroy all relate to the contact tracing, whatever form that may take relating to individuals and other individuals who may have self-identified, that is very personal information. It resides with the individual. And I don't think that should be part of a massive database that is not under the control of the government. I just reject that proposition. That doesn't mean there's not going to be a lot of valuable data that public health authorities have that there's tons of data now on. Of course, all the people who have been diagnosed as COVID-19 positive and how long it takes them to recover and the conditions under which vaccines are being worked on. Now there there's a ton of data being developed. The only part I'm advocating that we delete after it's over is the part relating to the contact tracing.
It's as Apple said, they changed the name of their framework to exposure notification because the only intention of it was to make you determine if you've been exposed to it or someone and then seek the services you need. That's not going to be a particular value to others in terms of public health authorities. And they have already a ton of data. You have no idea under their possession. And you've heard of a chief medical officers of health everyday reporting on this. There is a myriad amounts of data, I assure you, that's not going to be deleted. I'm just talking about the stuff that is related to personally identifiable data of individuals who just want to find out if they come into contact and take the necessary action. I think that's perfectly respectable.

Vicki Lemieux [00:53:51] The challenge is always that, you know, we humans are endlessly imaginative. So once they get their hands on data, then they could figure out ways that they can use it to, you know, to analyze it and to prepare for the next pandemic. So you could see a scenario where there's a public health argument for saying, well, we want to study patterns of interaction which lead to the spread of this disease.

Vicki Lemieux [00:54:22] And so whilst you could say, you know, this is very sensitive information, as is your genomic sequence, your protein, you know, your proteins, there's there's many, many aspects of health related data that are extremely sensitive. But you could make an argument to say, well, this will help us understand how these diseases spread in future.

Ann Cavoukian [00:54:57] So if I can respond to that. I disagree. I bet there's always people always make the case for accessing identifiable data, and I'm sure it will be of value to someone.

Ann Cavoukian [00:55:05] But the risk to privacy is significant, and that's what makes it unacceptable. You have to understand the reference to letters that had been written. These are 300 academics and the epidemiologists globally from around the world in 26 countries wrote their first letter, which was also broadcast in The Guardian newspaper. It was amazing. They said it is simply intolerable. You will not have any success with his contact tracing. If privacy isn't paramount and totally protected. And I always just delighted with that letter. I've been tweeting about it. And yesterday another letter from one hundred and seventy other academics and epidemiologists etc saying essentially the same thing. I mean, it was so moving to me that these medical professionals would take the time to write this kind of amazing, amazing statement in support of privacy. And these are medical people. They know the value of data, but they also know the value of
freedom and how it can. It's just not going to work if you don't protect people's privacy. It's paramount. And I can't deviate from that.

Vicki Lemieux [00:56:20] So. Ann, can I drill down into that? That's amazing. And it's you know, it's unprecedented, quite frankly.

Vicki Lemieux [00:56:29] And I wondered, did they give a specific reason why they felt that the contact tracing, or whatever name we want to give exposure tracing, did they give a reason why they felt it wasn't going to work? Was it that they were invoking concerns about privacy in general, or were they saying that it was a collective action problem, that people wouldn't use it if they were concerned about privacy? What was the reason? What were they arguing in their letters?

Ann Cavoukian [00:57:10] Here's the one of The Guardian. OK, let me just if I may read is just one or two things. If public history in the UK, a public health body such as the NSH, builds centralized contact tracing apps that transmits superfluous data, they will struggle to win the trust of enough citizens to ensure the activity is suppressed. Such apps can otherwise be repurposed to enable unwarranted discrimination and surveillance. The letter said that it's crucial that citizens trust the applications in order to get sufficient updates to make a difference in tackling this crisis. It is absolutely vital that in coming out of the current crisis, we do not create a tool that enables large scale data collection on the population either now or at a later time. Thus, solutions which allow reconstructing invasive information about the population should be absolutely rejected without further discussion. And they go on and on. I mean, it's just so amazing that a group of these are a group of 300 experts have warned that digital contract terracing will fail unless governments build the technology in a way that strongly respects user privacy. So that just gives you gives you some of the idea of why they're doing this.

Vicki Lemieux [00:58:52] That's really, really fascinating. And thank you for bringing those letters to our to our collective attention. And we've reached the time allotted for your intervention, Ann.

Vicki Lemieux [00:59:06] But thank you very much to getting us off to a really fascinating and thought-provoking start. You're always spot on in this this area. So I look forward to exploring your ideas further as we as we move forward our next lead witness.

Ann Cavoukian [00:59:26] If they have questions, people can email me. I always respond.

Vicki Lemieux [00:59:46] Okay. Thank you so much. Thank you for joining us.
Lili Liu

Vicki Lemieux [01:00:17] I'm going to turn it over to you now to present your thoughts.

Lili Liu [01:00:17] Okay. Thank you.

Lili Liu [01:00:43] My presentation takes a different perspective on the privacy legislation and how its interpretation or application seems to be limiting or restricting what we can do to help older adults living with dementia, who wander and are risk for going missing. It is estimated there are over half a million Canadians who are living with dementia. And annually we're seeing about 25,000 new cases. In about 10 years, we estimate that this population is going to increase by 66 percent to nearly a million. It is estimated that 60 percent of people who are living with dementia will wander and get lost in. The source of this statistic is unclear and the stats we do have are outdated. We do not know how many get lost for the first time nor do we have accurate numbers on how many older adults with dementia repeatedly go missing. We also do not know how many are returned home safely. But what we do know is, as progressive dementia is age-related, the prevalence and incidence of this condition is going to increase with population aging. We know that the number of older adults who go missing among men and women is increasing each year, but that's about all the statistics that we're able to get from police services. The reason we do not know how many of these cases are due to cognitive decline or dementia-related wandering is because police services do not share this information on account of the privacy legislation. While certain police services do collect detailed data for their own purpose, they do not think that they can share that data with researchers, with public health, with policymakers, nor other policy services because cognitive impairment or dementia is considered health data and protected by privacy legislation. This poses a number of challenges.

First, community programs such as Alzheimer's societies are unable to plan for capacity to address the issue of increasing numbers of older adults who go missing. Second, first responders, including police services, are also unable to plan for capacity to address the needs of this population. We know that certain police services have data that shows
there's an escalating number of seniors who go missing. For example, the Toronto Police Service report, six older adults are reported go missing on a daily basis, and this doesn't include those not reported. So with respect to allocating resources to address this issue, the need is increasing. Third, there are innovators of technologies that use surveillance, and program designers, are unable to implement solutions because they do not have accurate data on the trends and true numbers of older adults with dementia-related wandering at risk of going missing.

Lili Liu [01:03:53] Search and rescue teams and first responders. Vulnerable persons registries are typically incomplete.

Lili Liu [01:04:03] Often, persons who go missing are not in the registries, and existing data may be outdated for those who are registered. These registries are also owned by specific services such as a local or regional service and not all search and rescue services have access to them. Therefore, vulnerable persons registries do not necessarily speed up search and rescue efforts. Without quick access to basic identification data that is current about a missing person, there is a delay in the search for someone who is at risk for injuries or death.

So what's happening during the COVID-19 pandemic with this population? We don't have data, but we can surmise that older adults who wander, still need to move about safely, because the behavior of wandering often stems from the need to deal with agitation or are related to behavioral issues. The pandemic lockdown to contain the infection makes it more challenging for people with dementia to leave their rooms or their homes, especially when there is no contact with family, volunteers and reduced staff to accompany them on outings.

The risks for residents leaving facilities unaccompanied is as real as ever. People with dementia who are living in the community may not understand the concept of physical distancing, and so they may continue with their routines and become disoriented when public transit is less frequent or there are fewer people willing to assist them. My research team and I believe more than ever there is a need for technologies that can monitor, locate and share basic minimal information about vulnerable older adults, in order to in order to keep them safe and to locate them when they do go missing. Currently, the response time is too long. Our team sees self-sovereign identity, or SSI, through technology such as block chain, as brought up earlier by Ann, as a solution. This decentralized model can allow us to speed up the search and rescue process when a person goes missing.
A complication is, of course, the consent process with individuals who have a cognitive impairment. If a person is in the early stages of dementia, the person could participate in giving consent and in identifying guardian(s) who can make decisions related to SSI when the person is no longer able to. Guardians would be a part of this self-sovereign identity solution. To finish, I pose the questions: How do we balance privacy with the need to release personal data that speeds up location and safe returns of our vulnerable older adult population with cognitive impairment? And how do we address consent in persons living with impairment who may or may not have guardians?

Vicki Lemieux [01:07:04] Thank you so much, Lili.

Vicki Lemieux [01:07:05] That those two questions were well, I actually posted one of those questions to the chat for you, because I think, you know, you you mentioned a very analogous public health situation where, you know, there's a lot of very sensitive data that's being gathered, obviously on on these individuals with Alzheimer's and cognitive impairment. And, you know, in the context of COVID-19 as well as outside of it and the kind of information that's needed to to track and trace if individuals go missing. Very, very analogous. And yet this is very sensitive information. So we have again here a situation where you could make the justification for using this data, collecting this data on public health grounds on the grounds of protecting these individuals. And yet, you know, is it a step too far? Is is that information too sensitive to to be gathered? So I guess, you know, what's starting to emerge is what kinds of frameworks might we use to make those kinds of decisions. So I've got some questions in the chat here or comment from Nadia, who says, in my view, it depends on who uses the data and the purpose or in the parlance of the Health Information Portability and Accountability Act HIPA, a meaningful use.

Vicki Lemieux [01:08:33] I have difficulty with the notion of warranted because it's very dependent on context. Warranted, was a term that that I used in my question. So I just wondered if you had any thoughts on that. So does it come down to the purpose and meaningful use? What framework do you have in mind when you're thinking about this data?

Lili Liu [01:08:57] I think this really depends on the location or geographic location in which one lives, and what legislation is in place there. I think not all privacy legislations are the same around the world, nor are they interpreted in the same ways. We did a project where we tried to deploy an app that was developed in Canada and we wanted to engage community citizens to participate. Community volunteers participate in helping locate missing persons with basic information, including a picture of the missing person, they access through a mobile app. The idea is that volunteers would be “extra
eyes” on the ground to report if they spot a missing person; volunteers would not be in roles of search and rescue personnel as they are not trained.

Lili Liu [01:09:51] This concept of a mobile app that engaged community citizens who volunteer to be on the look-out for missing persons within specific geographic distanced arose from our observations that often, when a senior is reported missing, community members come forward to reveal that they had seen the missing person but did not know he or she was lost. Eventually, missing seniors are found either severely injured or unfortunately passed away.

Unlike missing children, it is not always evident that older adult is lost. Even when we suspect someone is lost, we tend to respect one’s privacy, we tend not to approach them to offer help. A challenge we faced was that this form of alert would have to be triggered by police services after they consult their vulnerable persons registries, interview the family or care partners, and rule out foul play. This removed the advantage we initially thought could be gained if community volunteers could receive data pushed out by care partners as soon as they noticed a loved one went missing.

A similar alert system that uses a community app is currently being used in Scotland; it is called the Purple Alert. This system does not go through the police services, instead it is triggered by community citizens and operates out of Alzheimer Scotland, a community organization. They engage the community. They don't seem to have an issue with engaging public citizens in volunteering, signing up for this app and then using it. Subscription downloads now exceed 10,000. We are interested in working with them to assess the impact and effectiveness of this approach. Although the general principles of privacy, security, of personal information applies, here is an example where geographic location and interpretation of privacy legislation may vary.

Lili Liu [01:11:23] And this is why we're very interested in SSI. Towards the end of today, Noelannah Neubauer will talk about our SSI project, which we relate to the issue of persons living with dementia at risk of going missing.

Vicki Lemieux [01:11:32] Yeah, yeah. So there is a there's a question from Kohei about, you know, your plans to to encourage the use of SSI. I don't know if you want to say anything more about that right now.

Lili Liu [01:11:47] Yes, Noelannah, will present on that specifically.

Lili Liu [01:11:50] But what I will say now is the very first stage of this project that has just finished. I really like how Ann described SSI.
Lili Liu [01:12:03] Self-sovereign identity and what it means to have our data decentralized, but the first phase of this Noelannah has been doing is just to try and communicate with the end user. The focus was on how to communicate the concept of self-sovereign identity with older adults who have progressive dementia and their care partners.

Lili Liu [01:12:19] What this mouthful of terminology actually means. I think the concept and terminology pretty high level and difficult for everyday citizens to understand, let alone your older population and those with cognitive impairment. So finding the language to communicate is the first step actually.

Vicki Lemieux [01:12:42] So an interesting question is coming in from Twitter too, which you maybe can’t really respond to. But just to take note of, how can we best respond to privacy activists when trying to eliminate some of the privacy restrictions to better help people with dementia? And that is the core question that your research is really trying to address.


Lili Liu [01:13:10] And just by way of an example, what we mean by minimal and just barely necessary information does depend on the context.

Lili Liu [01:13:19] If it's the information needed to locate someone, then a photo, something that’s current that describes if they were using a walking device, that sort of thing is helpful. The care partners often have the most up to date information and they would participate in releasing that information. However, that most up to date description is personal and identifying information. But that is precisely what is needed in order to locate someone missing. Once the person is located, that information is removed. The technology needs to ensure that personal identifying data is not kept. That is the balance that we are trying to work with. As it stands now, it's not working if we strictly abide by a black and white interpretation of the privacy legislation. Context, protection of the data and consent all need to be considered. I appreciate the feedback and the suggestions that have been offered.

Vicki Lemieux [01:14:04] Thank you so much, Lili. It's wonderful to have you here. And I know that you've squeezed this into a very hectic, hectic schedule. So thanks. Thanks very much again for joining us. And we hope that you can stay for or rejoin as time permits. But for now, we're going to switch over to Jennifer Pougnet. So, Jennifer, thank you so much for being here, because it's very late in the day where you are. And so I'm
All right. Well, hi, everyone. As Vicki introduced. My name’s Jennifer Pougnet. Thank you for having me today. I'm excited to learn from the lead witnesses and as others have stated your questions and our discussions during this innovative session. My discussion will probably take a couple steps back from the sophistication of the previous presenters. But really today I'd like to share my perspective on if governments can respond to COVID-19 and still respect the privacy of the individual. My opinion on this is yes.

But governments could do this or it would be easier for governments to do this if there were stronger data and digital ecosystems already in place that ensure privacy and data are protected and proactively considered in times of crisis.

Efforts around the world are highlighting how data ecosystems are enabling more effective response to COVID-19 in some countries. However, in other countries, the lack of or gaps in their data ecosystems are hindering their response to this global health challenge.

It's really highlighting how we need to accelerate our efforts in digital transformation when considering data ecosystems and privacy. It's not an all or nothing discussion. There’s a time, place and conditions that can offer guidance when it is appropriate to share data and when it might not be. Additionally, data ecosystems should be governed by foundational data privacy principles. And finally, at a fundamental level, we should consider the distinction between data privacy and data protection. These are two separate things. Data privacy is to protect the rights of the individual to exercise autonomy over their data, whereas data protection ensures that data is exchanged in a secure way. These are both critical elements to a data ecosystem and an important distinction as it speaks to why data privacy laws and regulations should set the foundation for liberation of data to serve the benefit of society, as GDPR sets out, and why they should not be used to either hoard data or enable a surveillance state, as Ann was speaking to. COVID-19, is highlighting the need to strike a balance between closed hoarding of data and open data surveillance, towards data being used to serve both our citizens and the broader global community through data ecosystems. These data ecosystems should be governed by data principles such as respecting the rights of the individual ensuring they know data, what
data is being collected, for what purposes and by whom. That data privacy is being proactively considered in design through concepts like Dr. Ann Cavoukian's Privacy by Design.\(^4\)

Providing guidance on limitation of purpose and data minimization to ensure that data is only used for the intended purposes. And finally, anonymizing, pseudonymizing or aggregating data wherever possible. When it comes to data privacy, it's not an all or nothing discussion. There's a time and a place for sharing data. The Open Data Institute that Sir Tim Berners-Lee founded with Sir Nigel Shadbolt offers a tool called the Data Spectrum.\(^5\) It speaks to how data should be considered on a spectrum moving from closed to shared to open data. And this should be considered against the individual's wishes, the life cycle of the data and conditions under which it is to be shared or disclosed within a data ecosystem.

Jennifer Pougnet [01:18:39] Thinking about data in this way will help to achieve data serving the public good while ensuring data privacy and protection. In a post COVID world, we really can't go back to the status quo.

Jennifer Pougnet [01:18:54] We need to accelerate digital transformations across sectors to establish data ecosystems that incorporate privacy in both their design and their governance.

Jennifer Pougnet [01:19:05] This will enable more sustainable systems not only for countries citizens, but it will also enable more effective and efficient predictive analytics of and, if needed, response to future global health issues.

Jennifer Pougnet [01:19:21] Thank you for your time and the opportunity to share my perspective. I really look forward to your questions and our discussion, especially around the concept of what we do need to do post COVID so that we have those foundational systems in place so that we’re not having to scramble. I think that is my five minutes.

Vicki Lemieux [01:19:48] Jennifer, thank you very much for those reflections. And there are a couple of comments, questions in the chat.

---


Vicki Lemieux [01:19:59] So if you would take a look at that and just respond however you would like, I'd also just remind participants that you should post your questions to the Q&A section anonymously. So please do feel free to post your questions there.

Vicki Lemieux [01:20:21] And yes. So back over to you, Jennifer, to respond to the questions in the chat first.

Jennifer Pougnet [01:20:30] Wonderful. So the question from Vicki is, do you think governments have underinvested in digital and data ecosystems? And Nadia, one of the other panelists offered, in my view, governments have not maintained a sufficient level of data infrastructure and have not established responsive ecosystems. And I would actually agree with this. I spent a large majority of my time implementing electronic medical records in a large health system in Alberta.

Jennifer Pougnet [01:21:04] It was very interesting because we were able to technically do a lot of things.

Jennifer Pougnet [01:21:13] However, there was a lack of policy developed to actually enable the establishment of some of those systems.

And, some of the things that we’ve seen in the states, the value proposition of establishing a data ecosystem where we have connectivity under the right conditions, where it’s appropriate to be exchanging data for certain purposes was lost.

Jennifer Pougnet [01:21:40] to the focus on incremental change management, just adopting the EMR. And you saw that consistently whittled back. It’s a large investment. And it’s not actually viewed as an investment.

Jennifer Pougnet [01:21:53] It's viewed as a capital cost, which I really do hope post COVID that we will see a shift in that thinking that it is an investment not only in the health system, but in establishing sustainable structure or sustainable systems across sectors.

Jennifer Pougnet [01:22:12] Finland is a great example of a country that worked towards establishing across ministries, their data ecosystems, recognizing that they could better treat individuals, if they were to implement the connection of data sources from social ministries, education ministries to help inform that care. I think that has been something that has been under invested in and very slow going. The discussions I was having, many year ago in my first real job are still the same discussions we're having
today. I think it has been a slow discussion and slow progress. And I hope that this will accelerate back towards what we need to do.

Jennifer Pougnet [01:22:58] And then the privacy element will also help to move us forward from the two extremes, hoarding, hoarding data or data hugging, as Tim Berners-Lee references it, and a surveillance state. Showing that there is a way forward in the middle.

Vicki Lemieux [01:23:15] Well, you've raised some really important issues there in terms of especially switching from looking at this as a kind of a capital expense to looking at the investment as more strategic and also just part of the way that we live and do business.

Vicki Lemieux [01:23:34] Now, I think especially the transformations that we've seen with COVID-19 we've been talking about for a long time, but the virus has forced our hand in a way to make these transitions much more quickly than we would have really anticipated having to do this. And so if, you know, in thinking about, let's say, advice for someone like Minister Murray who opened the session, who's minister for digital government, what kinds of first steps, post pandemic or even, you know, as we can begin now as Ann Cavoukian was recommending, would you say that governments really should take.

Jennifer Pougnet [01:24:23] I would think that investment in the infrastructure element needs to be considered first as an investment and an investment in the future of a country, and that investment is done in a thoughtful way when it considers the governance of how that infrastructure is deployed and in the data ecosystems emerging from it; considering data privacy and protection, considering what governance looks like to enable the sharing in those ecosystems and really considering another two elements that I didn't really speak to but are definitely emerging in the context of COVID, are establishing data standards in terms of data quality and interoperability. Recognizing that if we want that data to be of value to inform services that governments are delivering, it needs to be of a high quality and it needs to be interoperable with other data sources so that we can get the most value out of that data for those purposes. I think that's something like the World Health Organization is coming under attack for. And I don't think it's a reason not to invest. It's a reason to invest in high quality infrastructure to enable that high-quality data capture.

Vicki Lemieux [01:25:39] You know, you don't have to respond to this, Jennifer, but just when you talked about interoperability, it brought to mind the kind of the double edged sword of interoperability in terms of data use and data privacy, because oftentimes it's
the ability to make data interoperable that allows for the aggregation, the creation of data sets on individuals that can lead to reidentification, for example, in the context of health care.

Vicki Lemieux [01:26:11] And so, I mean, do you agree that there's a double edged sword there? We want interoperable data because it's more useful for us. But on the other hand, when we start to make data more interoperable and share data across, say, government ministries or departments and even across governments, do we run a greater risk of privacy breach. Do you see that tension there? Do you agree with it?

Jennifer Pougnet [01:26:42] Yeah, absolutely I do see that tension.

Jennifer Pougnet [01:26:44] But I do believe it is possible to move towards a reality like that. Where we're endeavoring to have that interoperability because whether or not we want to make it that way or not. I think it's already happening. A lot of the platforms, Google and Facebook, already are making that data available to overlay it with other data, it's actually already quite easy for those who have the knowledge and know how to actually execute. So that risk of re-identification is becoming more real every day, whether or not we're working towards using that for the purpose of optimizing services for citizens. That being said, I think that's why it really needs to be established very solidly and fundamentally within privacy principles. Making sure that governance accounts for data minimization; data is only used in for the intended purpose that is set out within that data ecosystem and other elements like data anonymization, pseudonymization, and aggregation are or deployed wherever feasible. Governments are trying to achieve, I think that sort of aligns with Ann's last comment around if we eliminate all the data, we lose the opportunity to learn from it. And it's just that identifiable piece. So wherever we can get data sets together that we can learn from without that risk is key, right?

Vicki Lemieux [01:28:17] Yes. I think that that is a great place to end your presentation. And thank you for raising some really important points in your reflection. So I would just like to invite Robin Renwick, who is our next presenter.

Vicki Lemieux [01:28:40] ... I'm going to turn it over to Robin for your reflections. And you're coming to us from which part of the world?

Robin Renwick

Robin Renwick [01:28:40] I'm in Ireland.
Vicki Lemieux [01:28:40] Thank you very much for joining us. And hope hopefully it's not getting too late for you there right now.

Robin Renwick [01:29:09] No, it's not too late. And. And thanks, Victoria, for the introduction. Good morning. Good afternoon. And good evening to everybody, I guess. Some people further east than me. I'm going to dive right in. We all know that five minutes, is not really that long. And I am just going to state my position. And then hopefully that lead to some kind of fruitful and stimulating discussion. I think it's important to state that, you know, I think there's both the short answer and a long answer to the question posed, right?

The question posed, just to clarify is can governments respond to the COVID-19 pandemic and still respect personal privacy? I think the short answer is, is sort of humorous, right? It's slightly tongue in cheek, but I think it's representative of my own wider philosophy. And so you can situate the question posed by turning to the two popular adages, which are really both just kind of variations on the same theme. Right. So the first is Betteridge is Law, which is also known as the Law of Headlines, which basically states that if any headline ends in a question mark, the question, can inevitably be answered with the word no.

Robin Renwick [01:30:24] And then in a similar vein you have Hinchcliffe's law, which states that if an academic paper title is phrased by a question.

Robin Renwick [01:30:30] The answer outlined in the body of the paper is also invariably a no. So that's the short answer dealt with. But I'm going to put that aside because look, I think it's fair to say that, you know, the short answer is a little bit to reductionist. And it doesn't really depict the complex nature of the question or the discussion that is needed, the nuanced discussion that is needed to fully understand, A, what the problem actually is and B, what the solution to the problem may or may not be. Over the weekend as I was preparing for the seminar, as you do, you know, I looked at the question and realized that the question itself is a bit problematic. Right. And this sort of clouded the situation.

Like the first issue is that I don't think I understand what personal privacy is or even what it's supposed to be. Right. And that's not to say that I haven't studied privacy, nor is it to say that I don't have experience and expertise in thinking about what it may or may not mean in this context. I think if you talk to most privacy experts, academics, privacy practitioners, they're pretty much all agreed. The privacy in itself is extremely complex construct and there's no one size fits all description and there's no cache all
definition. And even if you think about the construct, it usually morphs and evolves and changes with respect to person, place, situation, culture and context. Right. And it even seems to morph and change with respect to time and space. OK, so I'll give you an example from my own personal context. And you can see this is as an analogy, if you like. Right. And like I'm a pretty private person and I'm quite lucky because I live in a lovely cottage in rural southeast Ireland. I have very few neighbors and there are relatively few people around where I live. But when I go into my bedroom, I still sometimes close the curtain that covers the bedroom window. Well, funnily enough, I don't close the curtain every time in my bedroom. It sort of depends on what I'm doing at the moment. It depends on what I think I might be doing the near future. It depends on what time of the day it is. It depends on what time of the night it is. Sometimes it even depends what day the week it is. Right.

But even funnier is that my privacy preferences sort of changed in light of the current COVID situation, and that's because there are more people passing my house, because they live within the 2km radius that they're allowed exercise in. So people are using the road as a kind of the daily exercise route. to make it even more complex. I share my house and my bedroom with my partner. Right. And she has her own set of privacy preferences. And sometimes we have to have a little negotiation about whether or not we think it's wise to draw the curtains or to close the curtains.

Robin Renwick [01:33:20] Now, OK.

Robin Renwick [01:33:23] That example is a little tongue in cheek, right. But it really just illustrates how complex privacy can be. And this is just a simple example of closing a curtain or not. I do think that it's really important to state and really an important distinction to make that for the most part myself and my partner are in control of whether the curtain remains open or closed, regardless of the situation we find ourselves in.

Robin Renwick [01:33:48] And regardless of the situation that is occurring outside my house and it's really, really important to maintain that distinction. So, I mean, I guess I can move away from that example and I can move to the first part of the question Right.

Robin Renwick [01:34:04] we can talk a little bit about what the perceived or the actual role of the government is in this current situation. And that's where the conversation gets a little bit even more complex. Right. Because I'm not sure if it's the sole responsibility of the government to respect my privacy. OK. There are other complicit parties, including those from the private sector. And actually, if you think about it more often than not, it's actually the private sector that have encroached on my privacy the most. Now, it's not entirely clear because it depends on what technology you're looking
at and what your jurisdiction you're looking at. But it seems that the technologies that
are being proposed would be provided by a combination of the public sector and the
private sector, as well as semi-state bodies, NGOs, private health service providers,
loss of dependent developers, phone manufacturers, telecoms providers and even
Internet service providers. But what that actually means is that there are a number of
perspectives, incentives and motivations. And I'm not even sure that given the current
situation, that everybody's on the same page. And if I don't know if everybody's on the
same page, we don't know what the potential impacts are going to be, because there's
no easy way to fairly, transparently or clearly outline what the impacts are if we don't
understand what everybody's goals and motivations are. So if you think about the
solutions proposed right, they more than likely have many moving parts that potentially
are going to cross multiple jurisdictions and multiple entities. And each of those entities
will have distinct roles and obligations and each of them will have their own ethical, legal
and economic frames to work from. And there's no easy way to make sure they're all
aligned. So to kind of sum up the technologies proposed undoubtedly have the potential
to have far reaching impacts not only on our privacy, but also in our fundamental rights
and freedoms. And so in my opinion, I don't believe the decisions should be taken
lightly, nor should decisions be rushed, regardless of how urgent we think the situation
is.

Robin Renwick [01:36:14] I also think that it's extremely important to openly and
transparently explain decisions that are being made to communicate what the potential
impacts are, so that citizens themselves can ascertain whether they feel the action is
being taken by the government are proportionate to the problem at hand.

Robin Renwick [01:36:32] And that essentially is the essence of maintaining trust, as
well as a healthy relationship between citizen and state.

Vicki Lemieux [01:36:43] Wonderful, thank you very much for those great reflections,
Robin, raising a number of really important fundamental issues for us to consider. So
I've posted a question relating to one of those fundamental issues around privacy itself.
As you pointed out, do we really know what we mean by privacy? So I don't know if you
care to reflect a little bit more on some of the ways that privacy is conceptualized since,
you know, since you are someone who has researched in that area quite considerably.
You may be aware that there are different conceptualizations of this. And the way that
it's conceptualized in legislation, you know, isn't necessarily the way that maybe we
should conceptualize of privacy or we that is helpful. And as Jennifer was pointing out
previously, there's a there's a difference between privacy and data protection. So
perhaps you could reflect a bit more on that.
Robin Renwick [01:37:53] Yeah I think it's pretty important to make the distinction between data protection and privacy. And then secondly, it needs to go back to your original point. I think it's nearly impossible to try and define privacy. I think you can frame it from a number of angles. You can frame it according to a number of frameworks or taxonomies. But to get that one size fits all description is extremely, extremely difficult. And not only that, I think it's important to note that that, you know, humans are kind of you know, bounded. You have suffer from bounded rationality most of the time, right. So it actually means that even though you thought you wouldn't, if somebody appraises and objectively, you're probably not making the best decisions. Like I'm happy to say that I'm quite a private person, but I think probably 70 percent of my Internet browsing is done using Google Chrome. Right, but I still think I'm a private person. And I think, you know, similar examples could be given by numerous individuals. So, you know, to answer your question, is there one lens that we should be viewing privacy through? I'm not aware of one. I don't think there will ever be one, because there's so many links to other kind of fundamental rights and freedoms, such as autonomy, liberty, security, and all those constructs in themselves that are immensely complex. But I do think it's important make the distinction between data protection and privacy and to try and understand and openly communicate the nuances of the conversation, because I think the nuances will always be there regardless of the situation.

Vicki Lemieux [01:39:36] Thank you. Yeah, you're right. Privacy is linked to so many, so many complex constructs in and of itself. One of the ones that has come up, you know, in the conversations we've had so far today is control.

Vicki Lemieux [01:39:54] You, yourself, mentioned it. You know, being able to control, make the choice of whether you open your curtain or you keep it closed.

Vicki Lemieux [01:40:03] And it came up in the conversation of self-sovereign identity as well. And I wonder if we should think about privacy as linked more to this notion of autonomy and control and being one's own agent. If that's a more helpful way to think about privacy than some of the more consequentialist definitions of privacy, like the bad things that could happen if your data comes out.

Robin Renwick [01:40:36] I think the link between privacy and identity is extremely complex. I don't have all the answers. I know that some of the discussions around self-sovereign identity discuss a lot of the notions of both data protection and of this kind of

---

idea of control over essentially their identity and then the credentials that touch their identity. And the only kind of guard that I would have or reservations I would have is that.

Robin Renwick [01:41:12] You cannot entirely be sure whether or not deployers of self-sovereign identity are playing by the rules. And I think that you might get into a situation where people are, you know, because there are actors that behave in a certain way. We've seen it in the open market where they may advertise their solution as being SSI compatible, but not actually deploying the application as it should be deployed. I'm not sure the best way to police that and it's certainly not the fault of the people who have developed the SSI backend.

Robin Renwick [01:41:50] It's actually more of a of a kind of inter jurisdictional problem within individual countries where maybe they don't have the right kind of regulatory framework surrounding the development of apps or the protection of personal data. Because, of course, you know, from my perspective in Europe, we have very strong regulatory framework in the GDPR are but not all countries have that. And I think that raises numerous questions regarding interoperability and, of course, data protection.

Vicki Lemieux [01:42:25] Yeah, yeah, we have a question from the Q&A here. I wondered if you wanted to respond.

Robin Renwick [01:42:33] I can have a look, let me see, I only see somebody asking why they can’t see the same chat

Vicki Lemieux [01:42:44] So I can read it out for you.


Vicki Lemieux [01:42:48] So I'm an identity expert leading the development of self-sovereign identity technologies via the Internet Identity Workshop. Did you have someone actually share how verifiable credentials and decentralized identifiers work?

Vicki Lemieux [01:43:06] So I'm not sure, you know, if the question is directed at you or, you know, just in general. I think this maybe speaks to the need for people to understand how these new technologies work. And maybe that is not something that the average person knows about or, you know, even some people involved in designing technologies. And this same individual is saying another problem is that privacy professionals rarely engage with learning about technology. So, do you see some of these challenges in in your own work?
Robin Renwick [01:43:47] Yeah, without a doubt. Like even in the conversations that I've had with the self-sovereign identity, folks at Sovrin. I've learned things within the last three or four weeks because I don't think that all self-sovereign identity deployments are the same. Essentially, they're making tradeoffs in different ways. And I do think, though, it's important to acknowledge two things. So I think it's important to say, OK. No system is going to be absolutely perfect. There will always be flaws in the system with regards to privacy and with regards to security. I think it's also really important to note that, well, from a European perspective, and this kind of links back to the, you know, the regulatory framework and the policy framework that is in place, hashed or encrypted data still is classified as pseudonymous data. As of now. OK. So if you have these hashes or encrypted blobs, let's say, being pushed to a network in some manner. There is always going to be a link that you may be able to use to re-identify the person. OK. Now, whether or not you can identify the person obviously comes down to the architecture of being deployed.

The second thing, let's say, and this is something I've thought about more quite recently because we've been involved in a couple of research projects, is that people need to realize that we're living in an age of machine learning and artificial intelligence leveraged data analytics. And I think over the next few years that's going to considerably change the game with respect to how far these data analytics firms or data on an entity could go in re-identifying subjects then trying to understand and gather meaning with respect to their transaction or behavioral data and then making links between the two. I think that yes, people have explained to me how things work. I think it is fair to say that a lot of the different identity systems work in different ways. It's hard sometimes to draw the lines regarding the similarities and the differences between all the technologies. And I think it's also important to state that none of the policy and legal frameworks regarding digital identity systems has really been set in line with some of the advancements of the decentralized identity management systems. So it's very hard to get an understanding of a where the lines are drawn and b how the existing technologies fit into or outside of the lines that regulators are thinking about being drawn.


Vicki Lemieux [01:46:33] That's all we are going to have time for in your intervention, but I hope you'll stay on the line to engage with the discussion as it moves on, because you've raised some really, really important issues specifically about technology. So thank you again for your reflections.
And I'd like to now turn it over to Chandana Unnithan. Chandana, are you on the line?

Vicki Lemieux [01:47:04] OK. Over to you. Thank you.

Chandana Unnithan

Chandana Unnithan [01:47:16] All right! Thanks to everyone who is present. And thank you, Vicki, for inviting me for this interesting seminar. I would like to draw from lead witnesses who spoke earlier and state my perspective.

Perspective Statement
First, I would begin with saying that technology can no doubt be such that privacy is preserved -- if designed suitably. During a public health crisis, the use of technology, how it is used, need to be communicated to all citizens, suitably. This statement is informed by my experiences from being a public health professional, digital health expert and also having worked with many digital enabling apps that support public health. And, I am also drawing on experiences from Australia.

Australian Experience – Contact Tracing
Chandana Unnithan [00:01:31] Many of you may be aware that in the COVID-19 crisis, how an app was launched in Australia. There has been much talk in the media.⁷

Chandana Unnithan [00:01:41] However, it has been proven that the appropriate use of technology and privacy preservation for public, is possible.

Chandana Unnithan [00:01:53] Tracking backwards from this pandemic time, it is not something that was achieved overnight in Australia. It has been in the making for many years.⁸

Chandana Unnithan [00:02:01] Initially, it was about implementing national e-health records and connecting all health-related systems.⁹ Having a connected health record

---


enables ease of support for every citizen, in times, such as a pandemic. There was indeed consultation with the public and the 'opt-out' option, in case a citizen did not wish to have a unified record. And very few opted out.

Second, there was a blockchain platform being used for transfer of data, drawn from the health record (with prior consent given by the user), and safely, for medical research. How was this achievable? All the data is stored and maintained within Australia only by approved government staff, on a certified protected cloud. Most importantly, citizens must have consented to make their data available for research, from e-health records. Researchers can perform queries only on the anonymized data. Third, most recently, the COVID-19 app was launched, which brought about much discussion about privacy in the media, globally.

Chandana Unnithan [00:02:28] Among many digital app deployments in Australia, the most important, is the transparent conversation with citizens. So, let us take this COVID Contact tracing app. To the common citizen, it was made clear on how the app works, how the data is collected with their consent only and how privacy will be protected. There were two levels of consent and it is entirely voluntary.

Chandana Unnithan [00:02:51] The second aspect would be to be looking at how the government actually makes a statement saying that how this data will be secure, how long it will be kept, how it is going to be used for only public health purposes. It was also interesting to note that a legislation has been enacted so that the protection of this particular data collected in the times of COVID-19, will be deleted at a particular time and it will not be made available even with a court order or to the police at any point of time, for any reason. This information was available on the public website, on the app and linked to all public facing communications (news, television, Internet). It was visible.

On another perspective, having worked with enabling public health technologies for long time, learning from the initial hiccups can help enhancements with public engagement.


Similarly, when new technologies emerge, may it be AI or blockchain – communication need to go out to citizens so that there is active participation and discussion. Any upgrades to current health systems also similarly need to be communicated, seamlessly, so that everyone is aware of the use of this technology and public can engage and contribute, effectively.

We are all going through a time of uncertainties and adding technology to it, without citizen’s active participation will only surmount concerns. So, it is very important, as the privacy commissioner and one of the lead witnesses, (Ann) has pointed out earlier, that technologies are designed for privacy preservation. It is also equally important for the citizens to actually understand, in a very plain and simple level, as to how a piece of technology is being used to protect our privacy. And if it is communicated in a simple manner - it has a lot of potential. That's my perspective as experienced in Australian context, using the living labs approach, which was also found to be applicable in the Canadian context of public health.  

**Current State-of-Play - Canada**

I would also like to comment on the applications that are currently out there and how some of them are being used in Canada. I am part of a private public partnership, Lifeguard Digital Health\(^\text{15}\) that is supporting opioid crisis with apps and has been successful in Canada. It is a proven example that you can preserve privacy and still save lives if it is done correct, in a transparent way. So that’s my perspective.

I'm happy to take questions or explain how it all works, as I have worn many hats in this field, from being an expert, technologist and public health professional. I have also done some work with Vicki and her team at UBC and the digital technology supercluster, on enabling the permission blockchain security for public health\(^\text{16}\) which holds significant promise, going forward.

Chandana Unnithan [00:06:30] Thank you.
Vicki Lemieux [00:06:33] Thank you so much, Chandana. I think we've got a question that came in on the chat. Or maybe if I could get you to take a look at the Q&A and then come back to the Zoom chat.

---


Chandana Unnithan [00:06:50] OK. The question is “how can we ensure that individual health data is publicly protected and anonymous, but simultaneously those digital entities can be lost or deleted?”

Chandana Unnithan [00:07:06] This is a question that probably requires a very long answer and cannot be answered within this time slot. Short answer - it is possible to do this. It’s a question of balancing anonymity and use of right technologies, as well as legislation. I had spoken about an example from Australia earlier.

Vicki Lemieux [00:07:41] OK, I posted a question or there’s a couple of questions on the chat. So maybe you could tackle those ones if you feel that those are questions you want to respond to.

Chandana Unnithan [00:07:58] Okay, looking at this question, “what are the some of the key strategies for deploying the technology that respects privacy and what are the characters that define the privacy?”

Permission Blockchain
Chandana Unnithan [00:08:08] That is a question that takes us to using permission blockchain. I could probably explain both at the same time. From my experience, blockchain technology use can be designed with effective participation of people, so that they become champions, and propagate the knowledge further with peers. And this strategy of citizen engagement and participation, always have worked.

Chandana Unnithan [00:08:56] And it is essentially by involving users saying who will they permit to use their access to information. And for governments to explain the methods and legislation that is available to protect their privacy, and how it is done using technology. And once there is consent, it is informed consent, citizen buy-in - which can then be utilized for their own health protection in times such as this pandemic.

Senior-Care/Dementia Care
And going back to one of the lead witnesses earlier, where we looked at dementia care. A combination of apps, legislation and participation can be used to really trace people lost in transit (as they wander out of care homes). For example, obtain their consent to be tracked when they are fully aware, and explain to them as to why it is being done. Alternatively, explain this to the carers if the person is already in the dementia care situation. And this way, the technology can be effectively designed with informed consent and used to protect their lives.
Chandana Unnithan [00:09:42] So. It's a question of transparency - in a very short answer.

Vicki Lemieux [00:09:51] Yeah. Great. There's not a lot of time to drill down into the fairly complex technologies. We've got a couple more minutes before we have to move on. Is there anything you would might want to add based on any of the other questions or comments on the chat?

Citizen Engagement with Privacy

Chandana Unnithan [00:10:12] OK, so one of the questions here is, 'do you think that citizens make different calculations about how much data are shared under different circumstances?'

Chandana Unnithan [00:10:21] We all do. I would agree with that. And I do think it is a question of how much of data is shared, under what circumstances.

Chandana Unnithan [00:10:30] It is a question of obviously the individual privacy. And how important is this in this context? For every government, it would be a different, but it is still a public health crisis now. We have to recognize the gravity of this situation and look for the common good in a health crisis, no doubt, with informed participation.

Chandana Unnithan [00:10:46] It would essentially depend on the situation in a public health crisis when lives are really at stake.

Chandana Unnithan [00:10:54] Really, it is about saving lives.

Chandana Unnithan [00:10:58] That's a little more important. COVID is unlike any other crisis that we have seen in recent history.

Chandana Unnithan [00:11:05] Protection of privacy is of prime importance, but equally important is saving lives in a crisis. Both cannot be compromised. Thank you.

Knowledge Translation for governments

Vicki Lemieux [00:11:20] Yeah, so this kind of begs the question for me. I mean, you know, as you've pointed out, people make different calculations. And it's really important about context and different countries have different concepts and contexts and relationships with their citizens. So the question that's really coming to my mind: can we learn from what you know, from one another? What is done in Australia with a different
context and a different relationship between citizens and government? Is it possible to just take that solution and transplant it to another jurisdiction? Let’s say it is. You know, we looked at technologies that are being rolled out in Asia, for example, and how the technologies are being used there. Is it possible to take those technologies and transplant them in another jurisdiction?

Chandana Unnithan [00:12:22] This is a very good question and moot point. My perspective on Australian experience and knowledge is almost immediately transplantable in Canada. It’s just a question of how much do people out there really are aware of what is being done by provincial government or federal government in Canada? How much is communicated to the public as to the technology, and how it is being used? As the Australian experience stands testimony, if it is really made transparent to the public, and citizens are engaged, there will be no doubt enabling solutions for helping everyone.

With regard to other Asian countries, there might be cultural differences in terms of how public health surveillance is done and how these inform legislation. Australia and Canada are very similar culturally, the way we work in the public health systems, and being commonwealth nations. What would apply in terms of privacy protocols and cultural values that inform legislation, would no doubt be applicable in the Canadian context. It would be very useful to learn from each other. This is my informed opinion also as an Australian, living and working in Canada for some time and also having translated some experiences to both countries in the UN COPUOS forum across the two countries.

Vicki Lemieux [00:13:27] Thank you. Thank you so much Chandana for the great reflections there and for sharing your perspective coming from the deep knowledge of the Australian context. It’s really fantastic to have that view.

So we’ll now move on to Ciara, Staunton. Ciara – are you there?

Ciara Staunton

Ciara Staunton [00:13:48] I am indeed. Hi, it’s Ciara.

Ciara Staunton [00:14:06] OK, great. And thank you for the invite to talk to you today. I’m coming from you currently from the west of Ireland. And I’m going to take the

---

conversation out a little bit broader to consider other technologies. We have had certain technologies which kind of grabbed the headlines, you know, a lot on contact tracing apps. But we also need to consider the right to privacy in the context of testing, treating, surveillance, the collections of samples and data for research, the creation of a COVID-19 biobank and subsequent sharing of all of this data across borders. Now at the outset, I do want to make two points.

We hear an awful lot about the public interest and the public interest in sharing data in this context. There is a clear public interest in testing, treating and sharing data for research and surveillance purposes for COVID-19. But there is also a very clear public interest in the protection of privacy. And the existence of this pandemic alone is not enough to justify measures that are going to limit your privacy. With each technology, any technology or process that may limit your privacy must be justified according to the principles of data protection. So it appeals to the public interest but still requires a balancing of the need to protect individual and public health with these other rights. That includes the right of privacy. But how this balance may be struck? What is it in the public interest? It's not static. And it very much evolves at the pandemic evolves. Now, the second point I want to make is following on from the question that you just posed is that context does matter in all areas of response from lockdowns to sharing of data and the use of digital technologies and context is essential in deciding how we may need to balance this public interest vs. right to privacy.

And in the particular context, we need to consider the spread and severity of the disease because it's very different in different countries, for example, in African countries compared to other European countries. We thought that there was going to this exponential rise of cases when in Africa, which we're currently not seeing even in the hotspots. The cases are relatively quite low. And we also need to consider the socio-economic factors that may affect the use of these technologies, particularly at issue, contact tracing apps, for example. There may be a lack of access to smartphones or there may be an older population which may not have the digital skills in order to get to the scale that was required for these technologies to work.

And I think it's also very, very important that when we're talking about, you know, Australia, Canada, Ireland, where I am currently in, there are some protections in place. But this is not the same the world over. For example, in South Africa where I do an awful lot of my own work, South Africa does have a data protection Act in place. It’s the Protection of Personal Information Act (POPIA) 2013 and was passed in June 2013, but it's not yet in force. We're seeing a rise in a lot of these digital technologies or the wide sharing of samples and data without this kind of robust framework in place. The final thing I will mention on the context is that there may be a real lack of trust in the state
who may be holding the data and in the research community, who may also be holding the data. And there may be real concerns, legitimate concerns about the future use of their personal data. Now, when we look at the risks that are involved in the sharing of data on the use of technologies there's a number of concerns that I would have with some of which have been highlighted for me. I would have the following concerns. I think the first one is that these approaches that we're talking about and these privacy encroaching approaches, they're part of a strategy to get us to this kind of new normal that we're talking about. But in using these strategies to get us to these new normal, there's a risk of normalizing them and normalizing limitations on the right to privacy or the limitations on data protection.

And I would have a concern that in getting us to the new normal, they in fact, become part of the new normal. Now we see these approaches, which are being developed for a particular purpose, which is in response to COVID-19, but again, there is the danger of function creep. And, I would have two concerns about this. The first is which has been mentioned before by previous witnesses. This is downstream uses of the technology. OK. Yes, it's used for contact tracing. Will they be then use for wider surveillance purposes or for some other different types of emergencies?

And the second point is, what are the downstream uses of the data and who will have access? Is it going to be the state that has access? And if so, what prevents us from using it in other contexts that we may not want them to be used for. And here, trust is key. Trust in the government. Trust in research, trust in the governance frameworks is a real world concern. There is also the concern that data will be used to further discriminate already marginalized groups. Now, we may see, again, coming back to kind of examples of the contract tracing apps for these immunity certificates or passports.

Are we talking about they may be voluntary on paper, but if they're going to be required to for us to go back to work, go to university, go into your shop. Are we being forced? Are they being forced upon us? And if we don't want to engage with them for various reasons, is that going to, in effect, limit our other rights such as a right to education or freedom of movement and so on? And then there are also two assumptions that when I'm reading a lot about this literature, you know, I'm not a tech person, I'm a legal academic. But there's an assumption that the digital tools are the solution when it's clear that it's just one part of a wider package of solutions and the testing and treatment strategy and that there's too much focus on the digital solutions, perhaps.

And then there's also your assumption that they're going to work when we're talking about the rollout of these technologies, when there's not the evidence that they are
actually going to work. When on a webinar, I think last week or the week before on this topic, someone described it as a social experiment. We are living in a worldwide social experiment on whether or not these are going to are going to work. And so if I’m going to conclude, I would strongly urge caution, I think which has been echoed through previous witnesses is that we cannot let emergency be used to limit the protection of privacy and our responses must be proportionate, transparent and justifiable. I think data and data impact assessments are key in any rollout or consideration even before we get to root out of any of these technologies. The processes and stakeholder engagement are key and this includes public engagement which is crucial for public trust. Yes, we are in an emergency, but we do have time for this. And I think the final point I would like to make is that any limitations and we are living in an era where there needs to be some limitations of privacy. They must be restricted to these exceptional, exceptional circumstances. Thank you.

Vicki Lemieux [00:21:33] Thank you so much, Ciara, for your very thoughtful remarks. And we have questions both in the chat and in the Q&A section, so I'm aware that we're running against time. So you could certainly choose to respond to any of the questions in either the chat or the Q&A as per your preference.

Ciara Staunton [00:22:00] OK. So I'm just going to see the first. And so engaging the public online e-Privacy is very challenging tips. I think so.

Ciara Staunton [00:22:09] Looking at the context which I work with in a lot from my research is in South Africa and across Africa generally. I think that there are already groups and processes which is already in place which you can start to engage with them. I'd be with you. Beyond that, literacy is a key concern. But I think if we start looking at patient groups or patient interest groups is a good way in which you actually start this. And this is not just with regards to the privacy, to the limits on privacy, but also all wide areas with regards to black towns, for example. There's been quite a bit of work with one group in South Africa, Sustain Livelihoods Foundation, and they have been actually trying to roll out a community engagement app in which to actually engage with a local community within South Africa on their views on various areas arm of the government response.

Ciara Staunton [00:23:07] “Can the technology still be effective if groups choose not to participate?” Well, if we’re going to look at it. I would think not, bias is an issue that we face in all areas, from AI and into other areas. But it's my understanding for these technologies to work, we need scale. We need everyone to get involved to meet with kind of like, you know, an all or nothing that either everyone is in or we have to look at some other alternatives.
Vicki Lemieux [00:25:08] ... So there is a question from Michael. Governments have imposed the lockdowns that are damaging economies and now they're proposing a violation of our civil liberties. Contact tracing as a means of getting back to normal. Can we trust them?

Ciara Staunton [00:25:30] I think this is very context dependent. I think, you know, a lot of governments, we have seen examples of governments which are using the emergency to for their own gain.

Ciara Staunton [00:25:42] You know, look at what's going on in Hungary. And they're using it to limit the rule of law. Whether or not we can trust them depends on the particular context. It depends on the trust that the local population has in its own government and also the reasons. It's also what are they using it for? Some of the issues: Is there a sunset clause? Is it going to be confined to this particular emergency? So very much again, going back to context, very much matters and whether or not we can trust them.

Vicki Lemieux [00:26:14] So at this point, I think we'll we'll pause there. So, again, thank you very much, Ciara, for raising a number of issues that we will continue to delve into and explore throughout.

Our next witness will be Holly. Could I just, though, pause to just remind our lead witnesses, our panelists, when you post your questions. Michelle has brought it to my attention that you're posting to all panelists. Could I ask you to post your questions or comments to all panelists and attendees so that those who are participating as just participants can also see your questions? And then that could stimulate more conversation.

So it should be all panelists and all attendees and then to the participants who are posting their questions on chat. They're asking, why doesn't chat work for you? Chat. It has been disabled for you for two reasons. Because we can't upvote questions on chat. And we felt that there would be a number of questions coming in from the participants because it's a much broader public audience. So we wanted to enable this capability of upvoting and also just remind you to protect your own privacy since none of you have necessarily consented to having your identities revealed. The lead witnesses have all have but participants haven't. Just to ask your questions anonymously as well. So being mindful of privacy. So hopefully that will help us all navigate this new digital world a little bit more effectively. So just remember the panelists post your questions to all panelists plus attendees for starters, and question and answer participants post questions
anonymously. And remember to upvote those questions that you’re really interested in hearing a response to.

OK, over to you. Now, Holly, and thank you again, Ciara, for joining us from all the way from Ireland and sharing your perspectives on privacy. Thank you.

Holly Longstaff

Holly Longstaff [00:28:34] OK, great. Thank you. I just want to say a few words about myself.

Holly Longstaff [00:28:39] Just so you know where I'm coming from here. So I'm Holly and I'm the director Privacy and Access PHSA research and new initiatives. So that's the Provincial Health Services Authority and my PhD and my professional work experience have all been around applied ethics, which, of course, includes privacy. And today, I'm going to be talking about data access and research use in the public health sector as it relates to innovation, because I want to make very clear to be very careful, that we don't conflate some of the other things that are going on in the time of COVID, like surveilling publics, with health research. And I also want to talk about the reality of data access and use, as well as the hoarding of data and the value of investing in data ecosystems that Jennifer talked about a little bit earlier. So I'm a public servant and I serve the research community across the PHSA. And just to give you an idea of what the PHSA is about. We're one of the largest academic health science organizations in Canada. So I serve over 700 researchers plus their staff and we cover a wide variety of research domains, including B.C. Cancer, the B.C. Center for Disease Control, which you may have been hearing about in the news lately, B.C. Children's Hospital, Emergency Health Services, Mental Health and Substance Use Services, Women's Hospital, Renal, Transplant, and prenatal services. You can see it's a wide variety of research domains.

And what I've learned in my job over the last three years is that getting access to data and sharing of data in the public health sector is incredibly difficult. Whether you have it with consent or without consent and with research ethics board approval, it's very, very difficult. And this has huge implications for the health of the patients that we all serve as well as the functioning of our systems, even under COVID. So since COVID hit, we've been able to innovate and transform with tremendous speed, things that would have taken years have now taken weeks and months. But I wonder why it took COVID. Why did it take a pandemic to foster this kind of change? Because inability to access data and willingness to share data and invest in research has always hurt patients. It's not just COVID patients. What about cancer patients? For a cancer patient, cancer is an emergency. What about kids with rare disease? You know, it was mentioned earlier.
What about adults living with cognitive impairments? And I'm just mentioning this because I really hope that we do not roll back in a post-COVID world when it comes to research and sharing of data with researchers.

So part of the problem stems from the fact that many of our systems within the public health care system in Canada were designed truly in an anti-research environment. So when something happens like COVID, it's not as easy as just flicking the switch and then suddenly we can share data. It just doesn't work that way. And data sharing is also incredibly political. So just to give you an idea what it's like really to work with my researchers in my community before COVID hit, after my people would get research ethics board approval and privacy approval and everything, it could take me months or years to get the data that my researchers required to do their work. And this is all after the Research Ethics Board has determined that their research is ethical and in the public interest. And in many cases, they never got the data that they needed to do their research. So I know that we are not doing everything that we ought to be doing with the data that we have.

And that suggests that we have a moral obligation to use the data that we have to improve our health care systems and to be a learning health system. And it can't always be with consent. So when consent is appropriate, certainly we need to do it a lot better than how we currently do consent. We know it doesn't work as well as it ought to. I did a little back of the envelope calculation this morning and I've reviewed thousands of studies as an ethicist on various research ethics boards and as a privacy person. And I can tell you, look, it's not uncommon to see a 60 page consent form or one clinical trial that has four or five consent forms associated with it. They are not participant centered. They are about liability. They are about protecting the institution. We know there's lots of research in bioethics that shows participants want interactive (consent) forms. They want the ability to skip over some information, dig into other information.

We know people aren't comprehending the consent forms the way they ought to. The other problem is that it's not an equitable process. We know that 80 to 90 percent of clinical trial participants for drug trials, for example, are white. Well, that's a problem because not everybody is white. And if you don't participate in research either because the informed consent process doesn't attract you or because your health authority is hoarding your data, you cannot benefit from research and you become a therapeutic orphan. And the people that you represent become therapeutic orphans in the future. But even if we could get consent right and we certainly need to do a much better job, we need to be able to use unconsented data to run our systems, to do all sorts of different kinds of research.
And I want us to think of a really extreme case where we might require consent for all research uses, and I want to show how that could have some negative and unintended consequences. So for example, if we had to use consent for every use of data, we'd probably have lots of breast cancer research and prostate cancer research. But what about basic science? What about research around STDs? What about research like quality improvement that tries to navigate how people ought to best move through an emergency room, for example? It's not very sexy, but it's vital to the functioning of our health care systems. I also personally think that there's a lot of room to innovate within the legal and regulatory constraints that we already have within Canada.

Certainly, our privacy acts need to be continually modernized and so does the tri-council policy statement that governs the ethical conduct of research with human subjects. Certainly, it needs to be modernized, but there's way more room to innovate than we're taking advantage of. And where that boundary is and where the tradeoffs are between when consent should be warranted and when it's appropriate to do a waiver of consent, that's something that's already problematized in our privacy laws and in the tri council policy statement. But the boundary needs to keep being negotiated through continual public engagement with publics and with patients. And that was mentioned by a number of speakers this morning already.

And I just want to close my five minutes by saying I want to echo what Minister Murray said at the beginning of our day today and that inaction is not value neutral. Acting has moral consequences, but so does inaction. And I personally think that if publics knew what we were not doing with data within the public health care system, there would be tremendous backlash and outrage. We could be saving a lot of money. We could be better distributing our limited resources and we could be helping our clinicians to benefit their patients.

Holly Longstaff [00:35:23] Well it's all in there.

Vicki Lemieux [00:35:27] Holly, thank you so much for your reflections. So at this point, I'm going to open it up to for you to take a look at the questions and the comments that have come on to the Zoom chat. And you can start with whatever questions and comments you would like to start with and respond to any that you feel you're able to.

Holly Longstaff [00:36:05] I'm gonna start with the shorter one from Yann that says research without, without consent is not a problem if it is not nonidentifiable for the type of fundamental research you meant--mentioned. It would seem that this that the access would often suffice. Is that not the case for the type of fundamental research I mentioned? It would seem that this.
Yann Joly [00:36:26] I mean, that that for type—I'm sorry, it's Yann. I mean, that for the type of fundamental research you were discussing.

Yann Joly [00:36:33] Maybe it's not always necessary to have access to identifiable data.

Holly Longstaff [00:36:33] Absolutely.

Yann Joly [00:36:33] There are some research where you'd advocate that you absolutely need even for fundamental research. You have research with identifiable data without consent.

Holly Longstaff [00:36:51] Yes. I yeah, I agree that most of the researchers that I work with certainly have no interest in accessing identifiable data. It's not all that useful to them. They want de-identified data and anonymized data and that's fine. But let me give you an example of where you may need identifiable data. And it's still justified by doing it without consent.

Holly Longstaff [00:37:09] I'm just going to use myself as an example. Last year, I got this horrible thing called Guillain-Barré syndrome. And it's something that you get after you get a virus or sometimes that can be caused by a vaccine in very rare cases. And it tricks your body into thinking that your body's part of the virus and attacks your peripheral nerves. Long story short, you end up paralyzed. So I was in a hospital for two months and had a robot arm picking me out of my bed and putting me in my wheelchair. I was very, very disabled for a number of months and I got some very aggressive treatment that was beyond standard of care from my six neurologists who were taking care of me. I recovered incredibly fast, much faster than anyone anticipated, fully recovered. And that's very, very rare.

I can promise you that nobody is going to benefit from my experience. No one is going to be able to access those data or biospecimens. I know. I work within the B.C. health care system and I know where my data are and I know where my biospecimens are. My cerebral spinal fluid, the rest of it. No one will ever benefit because our notion of privacy is such that anything associated with a rare disease is considered just too identifiable to share. So in those cases, I think, look at COVID right now. We're in the middle of it and our researchers are in the middle of developing these vaccines. I bet they wish they knew a lot more about Guillain-Barré syndrome now. There's simply not enough known about it because there's not enough data sharing around a rare disease because of this fear of sharing potentially identifiable information. So that's an example where I think
you could justifiably override autonomy in some cases in order to achieve a big collective good.

Vicki Lemieux [00:38:56] Great. Thanks. Thank you, Holly. There are some more questions and comments in the chat. If you've got a couple more minutes. So if there's anything else you'd like to address.

Vicki Lemieux [00:38:56] ... So let me paraphrase. It might be easier just because it's hard to navigate. I'm seeing people struggle with it. So you mentioned I'm gonna ask you one about. Actually, that just came up in the course of your last response to Yann. You mentioned, you know, you work for the public health authorities, so you know where your data, your specimens are. But many citizens would not necessarily have that insider information that you have.

And so it comes back to transparency maybe as being a key to trust here? So would citizens—do you think that citizens would be more willing to share their data for scientific research purposes if they knew exactly where the data were housed, where the specimens were housed? How are they managed and handled on a granular basis? Or is that just too much to ask the average citizen? Like we're all busy and we have like enough cognitive overload. So is it just unrealistic to expect that citizens will necessarily take advantage of that information?

Holly Longstaff [00:40:34] Right. Well, that's an empirical question. And there's a lot of us at this event today who do research in this area, myself included. And what we found is that when we do, I'm part of a group led by Mike Burgess, Kim McGrail, Stuart Peacock and others who do deliberative democracy events. And we engage participants in Canada, the US, and abroad, about these very topics. And when we ask people about data and unconsented uses of data, they say, you know what? Yes, we understand the collective good here, but provided that it's governed appropriately. So instead of this individual individualistic notion of consent, they're really agreeing to consent to good governance. It's like we understand that these data are part of the health system and part of, you know, the treatments we receive and part of how the health care system functions. Well, we get all that, but we want to make sure that it's governed properly. So getting back to some of the earlier comments today, we have to make sure that we have secure research environments with good governance mechanisms, we need a lot of resources to be put into these great data ecosystems in order to serve the public good.

---

Holly Longstaff [00:41:37] That's what I think we have to do.

Vicki Lemieux [00:41:37] We have an interesting question on the Q&A, also mentioning that public health informatics has been drastically underfunded in comparison to the acute care sector. How do we increase investment in public health infrastructure and how do we address new technologies like social listening to impact on decisions like immunizing?

Holly Longstaff [00:42:06] Well, I think that I always encourage my researchers when we talk about these kinds of things, too, like there's lots of research going on in these areas. The research community understands the need for research. And I think now because of COVID everybody understands the need for research. We're not going to get out of this if they don't come up with some solutions for us. Researchers are going to be delivering the solutions. I think people get that now. Research isn't some side thing that people do off the side of their desk. This is the part of how our health care system functions and is integral to our health care system.

And so I think just talking more about that, being more transparent about that, having open, transparent communications with publics, I think will benefit everybody and having researchers really talk about the benefits of their work to the health care system. I always tell them, you know, talk to people, talk to your politicians about your great work. I think we need to kind of just change the narrative around research. And it's not just that secondary use (of data) that's, you know, optional. It's integral.

Vicki Lemieux [00:43:0] Thank you. That's great. So, Holly, I'm going to switch it over to Yann, now. Yann Joly, to bring us forward into the discussion. So, Yann, over to you.

Yann Joly

Yann Joly [00:43:30] Sure. So, I'm the research director of the Center of Genomics and Policy at McGill University. I'm also a legal scholar by trade who's been exposed much too long to multi-disciplinary scholarship for my legal training to really matter very much.

Yann Joly [00:43:48] I have carried out research, to give you a little bit about where I come from, investigating the legal and ethical challenge raised by modern medicine over the past 20 years or so. In the late 90s questions such as the development of the first genetic databases and a bit later the implementation of the electronic health record in the province of Quebec soon put privacy at the front and center of my agenda. So it's really like privacy kind of came to me rather than I had an interest in it, but it was soon front and center of my agenda.
And since then, I've been involved in developing and implementing several data access committee for biobanks at the national and international level. I'm actually currently involved in some of the various biobank and database initiative for COVID at both the provincial and federal level. I also teach medical confidentiality to students at the Faculty of Medicine at McGill University.

As I mentioned, I do have a fairly complex relationship with the notion of privacy. On one hand, I see the existence of privacy as a necessary precondition to respect of human dignity and also to secure the existence of trust in relationship. I mean, it is self-evident. I'm also a fervent believer in the importance of individual autonomy at a time where good citizenship and community values are sometimes softly programmed in us through the media and public policies, and that was even before COVID. However, I consider that major governments around the world at over the years consistently been unable to develop and implement truly satisfactory privacy regulations. Common weaknesses I've observed over the years include the complexity and opacity of the regulatory framework. And when I hear about this new notion of self-sovereign identity, I'm a little bit worried that we're not moving into an illusion of sovereignty in the sense of, you know, is just self-sovereign identity, really, truly accessible to a person with very limited skills in information technology, for example, and little interest in privacy. The slowness of adapting regulations to the online world we live in. It took forever for our laws to actually accept the fact that we weren't dealing with paper information anymore.

Questionable double standards depending on whether the rules are applicable to the public or private sector and a lack of nuance in applying privacy principles and tradeoffs to the medical context. We've heard Holly mention some of these really strange results that you sometime, you know, could get to by just applying privacy standards in the context of medical research were truly valuable research could be made impossible because of too formal application of privacy rules.

But sometime, it's the other way around where you see some really dubious research sneak by as well. And this sort of paradoxes is really well exemplified by the recent European general data protection regulation. While it's arguably one of the most advanced attempts at adapting privacy legislation to the virtual world, it is utterly incomprehensible to the non-initiates and I would argue to some of the initiates themselves. It's also intolerant of other legal orders and jurisdiction and broad to the point of fostering legal uncertainty on key aspects such as rule applicable to the secondary use of data for research purposes.
Talking about the challenges of protecting privacy in the medical context, already in 1982, Dr. Mark Siegler was observing in the Journal of the American Medical Association debt confidentiality no longer existed in the medical context.

Yet in 2019, we’re also hearing scientists at the same time complaining that abusive usage of privacy rules found in the GDPR, for example, is hindering important international research on genetic susceptibilities to the COVID virus. Again, this is the privacy paradox that we face with COVID-19, we are facing a situation quite unprecedented in contemporary times.

A public health emergency that threatens our most vulnerable and forces our most productive to change their work habits carrying the prospect of an economic recession. Surely dogmatic respect for dysfunctional privacy norms should not prevent our society to use the best technological means at its disposal to coherently, scientifically, fight the pandemic. However, such concerted strategy calls upon activities of research, health care and public health intervention that have very distinct implications and are governed by distinct ethical and privacy norms.

Yet reacting to the crisis with an overwhelming feeling of urgency, the boundary between these actions are becoming blurred, raising difficult questions, both for participants and practitioners on the ground and for regulators and policymakers. In such circumstances, privacy as an important role to play. It needs to ensure that the delicate balance between the desire of efficiently addressing the crisis for the benefit of the community does not disproportionately, arbitrarily, affect the personal lives of individuals leading to stigmatization, discrimination and loss of trust in the public authorities’ role in protecting the rights of individuals.

Recent examples of situation where this balancing act must be carried out about required disclosure, abound. For example, required disclosure of a small business employer about the status of an employee afflicted by COVID-19, or a collaborative initiative of researchers to efficiently create a biobank of COVID’s samples, both from the virus and from the human hosts of the virus to research ways to understand and prevent the disease. The interest of public health authorities to better monitor the spread of the disease and the compliance to public health measure using cell phones and tracking device. These are complex questions and I believe this is the first time they are seriously asked of us.

Don’t misunderstand me. Privacy regulations and ethical principles have existed for generations.
Yann Joly [00:50:55] Yet this is the first time that on a global scale we face a common problem that forces us to apply them and make these decisions. I see this as a unique opportunity for us to find new meaning and relevance for the notion of privacy, which has been under artificial respirator for decades now. How do we accomplish this?

Yann Joly [00:51:18] The key will be to carry out that balancing act in a concerted, pragmatic manner that will enable us to best address the pandemic without going too the extreme by fostering unnecessary abusive practices in the name of public health or at the other end by blocking beneficial innovative measures because of unclear and privacy requirements, I'm aware that this is much easier said than done and that the devil's in the details here.

Yann Joly [00:51:45] But importantly, we should be aware of the importance of the moment. How we define privacy to date, while we are facing COVID-19, could determine the place of the new privacy in the 21st century and beyond.

Yann Joly [00:51:59] Or it could chronicle the much-foreseen death of this notion. I for one, hope it will be the former. Thank you.

Vicki Lemieux [00:52:09] Thanks very much for the meaty ideas that you put forward in your presentation. So I've posted a couple of seed questions to the chat and, you know, feel free to respond to those questions or raise additional issues. Respond to other questions that have come up. I leave it up to your discretion as to how you want to take the conversation forward during your time leading.

Yann Joly [00:52:41] Sure. There's a there's a bunch of great questions there. So I'll start with your last question.

Yann Joly [00:52:52] So, are privacy laws simply not agile enough for a dynamic and sometimes chaotic world. What public interest versus privacy test would you suggest using to assess the issue?

Vicki Lemieux [00:53:06] So those are two separate questions.

Yann Joly [00:53:09] So the first the first one's really easy to answer. The second one's more complicated. The first one. Are privacy laws not agile enough? No, they're not. I would say law is rarely very agile. It's a problem that law has. And that's why we sometimes should rely a little bit more on ethics policies and other types of norms to do the job, especially when dealing with technology. So, yes, a lot of struggle and unless you have very innovative legislators, it’s often three steps behind.
What public interest versus privacy test would you suggest? I think it's an excellent question. I think this is really something we ought to think about. I don't have a test to propose right now, but I do think this is really an important question to address. Let me go back a little bit more on some of the questions. I see that. Michael McDonald. The question, don't health care data custodian have a responsibility to share relevant data with trustworthy researchers? What should the default position be here? That's an excellent question. I certainly don't think they feel that they have that responsibility. A lot of data health data custodians, especially if we are talking about either government agencies or hospitals in the province of Quebec, where I am from, have an almost sort of ownership relation with the data where really they have difficulty sharing it. It's very often, one, invoke privacy as a reason not to share the information. But when you get to the bottom of it, it rarely is a matter of privacy. Sometimes it's about competition. What do I gain out of the sharing? Sometimes it's about protecting from perceived liability that one could have in sharing the data. But it's really a misreading sometimes.

Other times, it really is that there are administrative policies that are extremely heavy that are preventing this sharing. So, I don't think there's a feeling that that health care custodians have this responsibility to share the data. I agree that they should certainly be advocate for health research as health care data custodian they should be advocate for better research, better healthcare at a time where we're talking about learning health care systems. They should certainly encourage secure sharing. I would definitely go with that.

Vicki Lemieux [00:56:12] Yann, thank you so much. I think that we'll leave it at that for now, Yann. There is a lot more to dig into what you have put on the table for us to consider. But let's continue the conversation. And you can come back in with further reflections and thoughts as we continue with Charles.... So, Charles, over to you. Thank you.

Charles Alessi

Charles Alessi [00:56:46] thank you very much for giving me this opportunity, because I think this is an incredibly important debate to start with. To give you just a bit of perspective as to who I am in terms of where I'm coming from. So I'm a physician, I'm a primary care physician, but I'm also Chief Clinical Officer of HIMSS, which is a global data and technology organization. So those are the perspectives. So I'm just going to address the potential conflict between privacy and the public, good as it's described, because in many respects it's nothing new. If we go back on very recently to the days of
HIV or even before the potential conflicts associated with patient confidentiality, all things which used to be involved in a whole host of conversations. And I'm quoting something from the General Medical Council now.

Charles Alessi [00:57:49] Patient confidentiality is a key tenet in all areas of medicine. However, circumstances exist. Confidentiality must be broken in the patients or society's best interests. It is permissible to overrule a patient's desire for anonymity where it could endanger the life of another health professional or patient.

Charles Alessi [00:58:10] Again, nothing new. And we used to deal with these issues on a regular basis and still do as physicians. However, the pandemic has really brought this into focus because governments have actually changed that case to case basis in terms of determining the merits of breaking confidentiality, which is really what we're talking about here all the time in terms of privacy as against the public good. Partly, I assume, because of their worries around managing the COVID epidemic and ensuring they protect the population. And and really, there are another couple of accelerants there which I think are being brought to bear.

Charles Alessi [00:59:03] One is the fact that we've moved to a blanket approach from a case to case approach, and we all understand that. Secondly, the fact that governments are really worried about a second wave, we know there's going to be a second wave of COVID or it's likely to be a second wave in COVID. And clearly the likelihood is that's going to come towards the light towards late to 2020s. In other words, in the fall or after. Plus, of course, the fact that it is likely that it will be accompanied by a flu epidemic. Hence the degree of urgency will increase even more.

And also by the observation that the countries that are used as the, you know, the poster boys and girls of how to manage a COVID response mean came from the far East, the Thai ones, the South Koreans, that Singapore was to a degree. And those were all notable in that they really were successful in managing the pandemic. They brought the they brought the walls down. They use community processes to ensure they managed social isolation. But also they were really quite, quite determined and very clear about the fact that the interests of the population completely was to be taken first. And in many respects, patients and citizens privacy was not necessarily considered to be quite as important.

We all heard about the contact tracing and tracking applications, digital applications. These countries used with a significant degree of success, I might add, to manage the spread of the pandemic, but also perhaps even more surprisingly, perhaps with the level of public support that they had in doing that and to a degree that was perhaps
unexpected. But in all those countries and I have actually interviewed people in each of those countries, it's really remarkable that the degree of public support was significant because people were really, really scared of the pandemic. So, again, it's clear, like everything else in life. This isn't a binary discussion whereby personal privacy is the most important at all costs because there are times when clearly managing a pandemic is as important and the responsibility of a citizen is also to the citizens around them.

So there is some balance here, but there are some issues which make me a little bit more worried. One that governments really like control when they're in power. And we've seen this year on year. Generation after generation. I mean, even something like income tax was first introduced in the United Kingdom under cover of the Napoleonic Wars by William Pitt the Younger in 1799, and really kept on being taken off and on and off until Robert Peel reinstituted it in 1842 when it's been there ever since. I'm not saying necessarily it's a bad thing, but things that are introduced in times of emergency, under emergency legislation, in times that are easy to introduce, but they're somewhat more difficult to remove. And there is a propensity to maintain them because there's always a reason why there are a really wonderful idea. So that's the first thing I think is it's worth reflecting upon.

And the second is around the value of data. Because in them, in our modern healthcare, which is a connected healthcare, where the care of individuals is the responsibility of a whole host of actors rather than purely a physician, it's a whole host of people that interact with citizens and patients. The only thing which really drives improvements in care is interoperability of data and also is the fact that people need to gain insights from the amount of data that's produced. So data really drives the health care system. So it's also something good to conclude.

Charles Alessi [01:03:37] I just wish to really develop a couple of issues because I think they're really very important. One is the sunset clauses. We heard all through this teleconference the importance of introducing sunset clauses.

Charles Alessi [01:03:55] I think they're really important and I'm a firm proponent of a sunset clause. These are extraordinary times and sometimes you have to use extraordinary methods to really manage a situation. But the sunset clause must always be there because the propensity, the temptation to retain that is great. That's the first thing. Secondly, it's some innovations which I've seen recently, which are absolutely fantastic. And I go back to the Apple Google application, which is really extraordinary in so far as a treaty maintains the privacy of the individual without using central servers. And I think that's great. I'm not saying that both organizations have not at some points, perhaps not being quite as open as they could be or others in the technology space
have always been doing. But clearly, this is something very good and I think it needs to be called out.

Thirdly, I think it's really, really important to talk more and more about the secondary use of data. We don't talk about that enough. We should talk about it more. There are some great examples globally. Organizations like FinData set up by the Finnish governments around how to use secondary data specifically for research are real examples. We can all learn from.

Charles Alessi [01:05:19] Fourthly. We need to be really quite clear that the old-fashioned types of consent are probably dead now we need to move to a far more dynamic process where consent is something which is which is, which is gained on a case by case basis. We tended to use consensus as being purely binary. You either have it for everything or you have it for nothing. I think there is a middle way. And finally, just a word about cyber security because it's all very well. We're worried about privacy and centralization, but there is a danger with COVID that cybersecurity is compromised.

And certainly, in all the conversations I've had globally, particularly in Europe. All the countries have highlighted the fact that cybersecurity attacks have increased exponentially during this period as more and more people have had to work remotely as more and more care has had to be delivered remotely. So that's basically the the points I wish to make. I'm now going to pass on to some of the questions, and I'll start with with Vicki. Can the site of interoperability of data the individual rather than the centralized database?


Charles Alessi [01:06:41] This is why the Apple Google initiative is so good, because it goes beyond the central database.

Charles Alessi [01:06:53] There's always a worry around central databases, especially if the government owns all governments control.

Charles Alessi [01:06:59] That's you know, not all governments are as benign as, as others. Some countries have a history of really trusting governments, while some other countries perhaps don't. So I think this is an important issue on anything which preserves the privacy of individuals is something which needs to, be needs to be really lauded. Another question, how can we ensure data sharing while protecting privacy to foster research as it evolves, as we discover which groups or individuals are more susceptible?
And this is a really good point. And thank you, Nora, for putting this point, because unless we gather those data points, how on earth are we going to start to develop the insights we need using artificial intelligence, using whatever we're using to ensure we then start to identify which individuals are they are the more susceptible to develop a corona virus in the second wave.

Now, how can we do this? I think we can do this by being as open as we possibly can about the use of data. And there are examples about being open around the use of data. The worries we have is that it will persist. As I said, in my view, these times are extraordinary. So perhaps we need extraordinary ways to manage this epidemic.

And the last question I'll answer is, “Do large commercial actors gain too much power over states to make independent decisions about privacy, even if they develop privacy respecting technology?” I'm thinking here about the danger of more monopolistic tendencies.

I couldn't agree more. Yes, that's true. Large, large commercial actors have too much power. That's very, very well known. Hence all the all the efforts being made now to clip the wings of some of these data integrators, which which, clearly have a significant amount of power and know a significant amount of information about us.

But actually, you know, if you take me, I use the Internet all the time. So these people, these actors already have that data about me.

So I'm less worried about them also being involved in a process of of mitigating the worst of the pandemic, because in many respects they have the data already. I potentially am more worried about a completely new actor being governmental or otherwise gaining access to that data as well.

I think there are moves afoot globally to actually manage that amount of information that these large organizations have and to ensure that it's appropriate. They clearly need levels of information, but perhaps they don't need to garner it in quite the way they garner it.

And I think there are some examples emerging of really responsible ways.
Charles Alessi [01:09:58] And this application that certainly is is one of them. It is unusual to hear so much in terms of support for an application. I mean, it's being adopted by most of the countries in Europe, the European Union and so forth, as it seems to have the support of people who would normally expect. The European Union isn't exactly well known for its support of these large commercial actors.

Charles Alessi [01:10:29] So thank you very much.

Vicki Lemieux [01:10:32] Charles, thank you so much, that was a really fantastic presentation and reflection on really fundamental questions that you've raised and coming from a deep place of, you know, being involved in the clinical practice and the research close the data that we're looking at today. So really, really appreciate your reflections. And I hope you'll be able to continue to stay with us to engage in the conversation. And very interesting that the Apple Google partnership, as you've said, has been mentioned a few times as a good example, because, as you say, it's rare to hear such an endorsement. So I would like to turn it now over to Nadia …

Nadia Diakun

Nadia Diakun [01:10:32] I am here. Yes,

Vicki Lemieux [01:10:32] Right. OK, over to you to take the conversation forward from where Charles left off.

Nadia Diakun [01:11:37] Charles is a hard act to follow. Good morning, good afternoon, good evening wherever you are on this planet. This is an immense and incredible opportunity to be able to speak to and hear from a lot of colleagues. In 2001, two weeks before 9/11, I was offered a position with the federal government of Canada in security intelligence. This was the first realization I had, that privacy really is moot. And that it really depends on a lot of things. I had the interview. I accepted the position. I came home and my son asked me very simple question. Did you take the job? I said, yes. “And now you don't exist,” he responded. Once you enter the world of security and intelligence, you become a fly on the wall, part of the wallpaper. Today, I am an ex-public servant, with my own startup on that came out of a Fintech: Future Commerce project through MIT in 2016.

Nadia Diakun [01:12:53] I cannot not argue that we as citizens are partners with government, and when there is a reaction toward anything that government does or intends to do. Once you have been a public servant, you know the gravitas of being
both citizen and public servant at the same time and having this dual responsibility. It really takes “two to tango” here. It takes us as citizens, and it takes a government to act. Fortunately for many of us, we are not vassals within our governments. We elect them, and we can un-elect them. We have voices. We can represent ourselves. We have others who represent us. The role of our government is to provide us with a social contract that we agree to. We accepted that social contract. We become citizens. We vote. The government is the provider of certain goods and services that benefit not just us individually, but also our communities, our cities, our provinces, our states, our towns. It is also the facilitator that we entrust with domestic and foreign policy and it is our representative on international affairs. So, to be really honest, I am very much a proponent of good government and good governance and many of us are very fortunate to be in such regimes where they don't take us for granted. Now to the question of this conversation that we're having: “Between a rock and a hard place: Can governments respond to the COVID-19 pandemic and still respect personal privacy?”

Nadia Diakun [01:14:24] What did you answer when you saw that question in your mind? I thought, yes, we can. We can.

Nadia Diakun [01:14:35] Today, we cannot do it fully. In future, we will be able to because the technology does exist. We can have privacy, security, interoperability, appropriate sharing of data for the good and that benefits of all humanity. First and foremost, we have to establish a very level playing field, 'very level', not just a 'level' playing field.

Nadia Diakun [01:15:02] I propose that this is what our level playing field is composed of. We must speak the same language. We have to use the same lexicon. We have to understand the lexicon and agree to the context. What does the word “privacy” mean? What does the word “sharing” mean? What does the word “identity” mean? We have various notions and we have various legal definitions. If we do not have the same lexicon, the same grammar, the same syntax and the same semantics and context, we will have difficulty in communicating. I think some of that has come up in the discussions and some of the things that we have heard today. This is such a complex area. There is no right. There is no wrong. There are middle grounds and there are difficulties and hard problems that have yet to be solved.

I do not disagree with any of the principles that have been espoused by previous speakers. In fact, I agree with many of them. But I do disagree with certain things. I disagree with “a scorched earth” approach to data, and what do we do with it after it has been collected. I believe that digital records should not necessarily be completely and totally purged. I do not believe in marketplaces where data should be sold. I do not
necessarily believe in financial incentives for data, because I know that many of these approaches could open doors for cyber security breaches, for deliberate criminality and as well as not necessarily good intentions.

Let's look at why I have this belief, because I need to defend myself here. History, archeology, geology. These are various sciences that we use to understand ourselves as humans. We look to anthropology to understand the communities that preceded us. We look to archeology to understand the human construct of this planet. We look to geology to understand the world around us. To understand other species that we share this planet with, we look at biology and chemistry. If we want to place ourselves somewhere in the universe, we look to physics. The sciences are always our source of truth.

Let us look at what would happen if we suddenly scrubbed every single scientific record we had. Would you agree that all church records that have been written from the Middle Ages on down should be destroyed because there is no real value to them today? I think not. Much of some of the conversation around GDPR are an Article Twelve, the one that says you have the—simplistically explained—as “the right to be forgotten" is really not quite accurate because I would counter anyone who says I have the right to be forgotten, perhaps we also have the right never to have been known. We cannot have the expectation of government to give us services and doing work for us, for our benefit as citizens, without mutual respect and mutual agreement.

I propose we can have both the record and the privacy. The technology is available. The foundation to make it real is not quite there. Its qualities are that it will be decentralized, distributed, transparent with confidentiality, integrity of the data availability, as the especially important, and weighted assurances we must have to make it real. That technology, simply put, is blockchain or the decentralized, distributed ledger. I will not go into the technicalities of it here because it is extremely complex. It is very elegant. The mathematics of it are extremely elegant. Safe to say that this could be literally the answer, which would allow us to share data, especially epidemiological data, health data without the consequences that we see and expect to see as breaches or violations of privacy, in future. We so much believed in that possibility in 2016.

Nadia Diakun [01:19:50] Now I’m going to send you the title of our paper. And I’ll send you the link so that you can download the paper.

Nadia Diakun [01:20:03] You can download the paper and have a read. In 2016, the Office of National Coordinator HealthIT in the United States Health and the National Institute for Standards and Technologies brought forward the very first blockchain
challenge. We were writing our capstone paper for the MIT Fintech: Future Commerce course. But we veered off from the commerce because very few of us were financiers. We had a greater interest in ethics, privacy law and the ability to share data, especially health data. And so, I convinced my colleagues, our team to put together a white paper and throw it into the pot for this competition. It is an interesting proposition to use technology that would assure the easy availability of health data, clinical trial data to researchers and to governments. Nothing would be revealed about the person who participated in the clinical trial. The complexity of it using homomorphic encryption is bit mind-boggling and it can take time to understand, that I can actually share data without revealing it and making it very open and very public. I think that this particular conversation during this time, at this rather unprecedented time of COVID-19, will lead to further conversations because the work is just barely beginning. We have many questions to answer. Questions of consent. Questions of availability. I hope this helps. I'll take any questions.

Vicki Lemieux [01:22:06] That's fantastic. Thank you so much, Nadia, and thank you also for sharing your paper. And I would encourage other lead witnesses, if you will excuse me, have papers that you would like to share. We're obviously delving into issues and topics that are quite complex. And we know, it is very difficult to address them all in the kind of depth that we would want in the short time that we have. So, I think there are some questions and comments that have been posted, or you can ignore all those comments and make other additional reflections. So, I just invite you to take conversation forward.

Nadia Diakun [01:22:47] Sure. Well, there's one in the Q&A, which is how do you download the paper? It doesn't seem to be downloadable and LinkedIn just brings up a reader. If you are having difficulties, please don't hesitate to send a little note on in. I will send you the paper via email or I'll make it available to UBC. And then, Vicki, if you have any requests for that paper, then by all means, please feel free to share because it is a public paper.


Nadia Diakun [01:23:20] Yes. Well, the question that is directly above is we have good government, but that can change quickly. And we have strong public interest now for data sharing. What should we be thinking about possible future conditions or is this less important? No, I don't think that it is less important. I think it is extremely important.

I don't even know how to phrase it, but to the neighbors next door - south of us - we have a rather curious administration. And especially in the United States, they desperately need a way and the mechanism to secure data and to make it public and transparent so that it is not manipulated for political expediency. The technology would certainly mitigate that. But before we even just leap to the technology, I, by no means, suggest that tomorrow we should all do blockchain. That is a solution. It needs to be framed and there has to be a very strong government infrastructure to develop an ecosystem with a very complex architecture, a digital architecture that underpins it. If we had these kinds of assurances through technology, then we could trust our governments regardless of who is in power because the data would be decentralized and distributed. There are many players in the game and “you cannot hide.” You cannot change the data. You can't manipulate it. It's simply mathematically impossible. And that is the kind of assurance that citizens can have.

Do I envision the commercialization of distributed blockchain health systems as many disparate systems from many individual providers serving different functions or one centralized system government that tracks everything?

No, actually. In our premise, we would like to see a very decentralized ecosystem.

So let me try to demonstrate this very simply. There are twenty-five of us online right now. Each of us is a healthcare provider or a hospital or perhaps an entity that is conducting clinical trials. Each one of us will be part of this ecosystem linked digitally through technical pipes and we would be able to participate in this permissioned ecosystem. One cannot come into it if you do not have real business inside the clinical trial area. You would have permission to be a participant. You would have duties and expectations to conduct not you as a person, but a machine, the computer that you're working from. And I'm not talking about a laptop. You would have permission to and responsibility to help maintain the data, process it, and keep the blockchain intact. This complexity of the chain itself requires a lot of compute power. Yes, it can be done in the cloud. Yes, it can be done in a secure the cloud. It cannot be a public cloud. It would have to be a protected cloud, a sequestered private cloud, that has been made cyber secure for the data.

On commercialization.

You know, private industry does have an interest in making money and profit because it does invest quite a bit and heavily into what it provides. But I would much rather see those to be open source equally distributed with all of the rights
and privileges and responsibilities that should go along with it, as well as the assurances that the mathematics and the encryption provides. I hope that answers the question.

Vicki Lemieux [01:27:36] So I think we are. How we doing for time? We have a few more minutes.

Nadia Diakun [01:27:44] I think I've reached the end of my time. But if you have a question to give or Vicki if I've missed something, please go right ahead.

Vicki Lemieux [01:27:51] Oh, my goodness. Well, there are so many topics to delve into. And it would be just lovely to have you speak for longer. But you're right.

Vicki Lemieux [01:28:00] We have reached the end of your segment. And we now have a slight pause just simply to get up and do a stretch to keep ourselves physically healthy for fifteen minutes. It's not much. So, let us break until noon and then we will return, and we will have Michael carry forward the conversation. So, thank you very much, Nadia. And to all of our lead witnesses who have participated thus far, it's been really fascinating to hear from all of you and the different perspectives that you have on this issue and the rich ideas and concepts to plumb and developments that you've brought forward. And so I'm deeply grateful to everyone so far and very much looking forward to the continuation of the conversation very shortly. So, let's pause and we'll come back in a in a few minutes.

Michael McDonald

Speaking as the eleventh speaker in this twenty speaker event, I feel like I have been in a long distance race, a “Zoom-a-thon” as it were, and that all of us need to pace ourselves to reach the finish line. To offer a somewhat different metaphor, it’s as if we were dining at a very rich banquet where we want to savour all the different courses. Each of us speaks from different disciplinary perspectives and experiences. And one value of this Witness event is that we can remind ourselves of the complexity of the issues that our lead question raises.

This links up with how we in ethics describe ethical judgements, namely as all things considered or integrative decision making in which all relevant factors – technical, social, economic, legal, environmental, etc. - are taken into consideration. This Witness event can be seen as an attempt to put on the table the multiple factors involved in making sound ethical judgements around pandemics and privacy.
My Background
To help frame my remarks I will, like the other speakers, say a bit about my perspective. There are three relevant aspects.

First, I've spent my fifty plus year academic career working in the area of ethics both on ethical theory and ethical practice. For a substantial part of my career I have focussed on the ethics of research involving humans. I was one of the principal architects of the *Tri Council Policy statement on the Ethical Conduct of Research Involving Humans.*\(^{19}\) However, I have been very critical of the way in which Canada and other jurisdictions around the world provide ethical oversight for research involving humans including the protection of research participants privacy.\(^{20}\) Research ethics boards (REBs) rely too much on front-end review of research applications and pay extraordinarily little attention to the impacts of research participation on participants.\(^{21}\) In other words, our REBs focus primarily on inputs rather than outputs or consequences of their decision making. We don't systematically gather information from participants about their experiences in research.\(^{22}\) So my colleagues and I have advocated for is an evidence based approach to research ethics.\(^{23}\) But there is a further crucial feature of my work here that deserves mention.

I have found that to gather information about the effects of research on participants, it is absolutely essential listen carefully, talk to, and learn from research participants.\(^{24}\) This is very relevant to our discussion today. We should be asking about the consequences of our policy recommendations regarding privacy in a time of pandemic and to do that it

---


is essential to engage in thoughtful and respectful dialogue with those people whose privacy we are trying to protect. In privacy protection as in other areas of policy making it is essential to take seriously the often quoted motto of the disability movement, “Not with us, without us.”

Second, I also come to this discussion as someone who has experience on a REB. I chair the Research Ethics Board for the Canadian Blood Services (CBS). CBS and our Québec counterpart Héma-Québec are major Canadian collectors of data and tissues related to transfusion, stem cells, and transplantation. CBS is then a major data custodian, and we on the REB play a central part in that role. But our object is not simply to gather and protect data but also to make sure that data is put to good use. CBS works with responsible researchers and research institutions in order to advance health research in areas relevant to our mandate. In this regard, I share many of the concerns expressed earlier today by Dr. Holly Longstaff about breaking down barriers to responsible data sharing.

Third, I have to say that I have so to speak “skin in this game” of privacy in a time of pandemic. My wife and I are in our late 70s and have compromised health conditions. We are members of that vulnerable population that you hear so much about. We very much want to see treatments and a vaccine for COVID-19 even if that requires sacrifice of some privacy on our part.

A Matter of Public Ethics

The central question posed today around governments coping with the COVID-19 pandemic while still protecting privacy is fundamentally one of public ethics. What is the right way to balance considerations of public health and personal privacy? How do we want our social institutions, whether in the public sector, private sector or not for profit sector, to behave? It’s a quintessential question right now about questions of public ethics. What is it that binds us together? What is it that makes us a community? COVID-19 has really posed this issue for us. It really poses a giant threat.

In the media the pandemic crisis has been labelled as a war. Many in the US and elsewhere who are inclined to conspiracy theories have tried to frame this as a war between nations. I think this is a dangerously distracting misdescription. Instead I would view this crisis as a collective challenge to the whole human species to protect ourselves.

In terms of the topic of this witness event, we are asking about the size and shape of each of our zones of privacy during and after COVID-19. Broadly speaking there are two predominant ethical theories underlying claims to privacy. One is individualistic
resting on claims to personal liberty. The other is communitarian centred on human flourishing as social beings. Both value privacy and its protection but in different ways. However, in a pandemic they come together in concluding that the zone of legitimate privacy must shrink during a public health emergency. This is because what we do and what happens to our bodies, in particular the viruses we carry with us, may adversely impact other people and our entire community. During COVID-19, each of us have legitimate interests in permitting and encouraging access to information about our health for developing preventative measures and treatments.

While COVID-19 is a global, species wide challenge, we can see profound differences in how different communities react. Contrast, for example, how the province of British Columbia specifically and Canada generally have responded to COVID-19 with our neighbours to the south. Of course, the differences reflect different kinds of leadership, but it also reflects different and divergent histories and social roots. Canada evolved from a colony to a self-governing state. The US began with a violent revolution. These are factors that are very much reflected in the different, albeit multi-faceted, cultures north and south of the Canada-US border. This is to say that the policy recommendations we make around COVID-19 and privacy have to be sensitive to the specific institutional and cultural contexts under consideration.

There is a further degree of specificity that needs to be taken into account, namely, diversity with specific jurisdictions. When, we talk about what the public wants or will accept, we have to recognize that there is not usually one public but many publics. In some of our discussions today, for example, we often spoke as if everyone had a smart phone and that protecting digital privacy while enhancing anonymized data collection for pandemic research and public health protection would address central issues. While this technological fix would be a major achievement, there is a risk of forgetting about the many populations even within Vancouver itself who are digitally disenfranchised. We need to remember we are dealing with diverse communities, in some cases very marginalized while in other cases very privileged. If we think of policy making as an exercise in building trust and trustworthy relationships it is essential for to take that diversity into account.

During this pandemic, those of us who work in areas where we act as health data custodians have a responsibility to protect the privacy of the people who provided that data, but also we also have a responsibility to promote the responsible usage of that data for addressing current and future health crises. And that means we have to be trustworthy data custodians. And what does that mean? I think ultimately it means that we have to view the people whose data we collect as not just data sources, but as an integral part of the data collection and data use process and governance. This means
more than providing information about data collection so that a digital box is checked off.

We need to find intelligent ways of meaningfully bringing citizens from across society into the process. We actually have to involve affected groups in the governance of our health data collection and use systems. Creating and maintaining the trust of those affected may well be both messy and difficult. But if we're going to have a public ethic that works here and balances legitimate interests in both individual and collective privacy, we need the involvement of the many publics involved. What I am suggesting here is quite similar to the movement to have patients involved as partners in health research.\(^\text{25}\)

And there are intelligent ways of doing this. My colleague professor Michael Burgess and my former student Dr. Holly Longstaff have conducted experiments and trials using citizen forums to look, for example, at biobanks.\(^\text{26}\) An earlier example would be Health Canada’s consultations around xenotransplantation (use of genetically modified animal organs for transplant into humans).\(^\text{27}\) These involve bringing together individuals demographically representative of a community to have expert informed but not expert dominated deliberations about the public policies needed for biobank operations and governance.\(^\text{28}\) The challenge then is to learn from and involve those whose data we want to use and to protect. In a free and democratic society, citizen involvement is essential for building and maintaining social institutions that are well informed and trustworthy.

Obviously, there are bad ways of getting citizen involvement. The highly polarized and toxic digital environments dominated by trolls, bots, and manipulative agents are a prime example. I am also familiar in my work with the manipulative use of patient

\(^{25}\) Don Willison and Michael McDonald, “Ethics Considerations When Involving Patients in Health Research”, Researching Together: Engaging Patients and Stakeholders in Health Research, from Topic Identification to Policy Change, Emily Zimmerman, ed. Sage Publications 2021


\(^{27}\) Edna Einsiedel, Assessing a controversial medical technology: Canadian public consultations on xenotransplantation, Public Understanding of Science, 11 (2002) 1-17

groups by pharmaceutical companies to promote their corporate interests. But as noted earlier there are also good ways of securing public involvement. And to return to a point I made earlier, the possibility of intelligent and constructive dialogue depends greatly on the cultural context or zeitgeist of the communities involved.

To sum up, in this Witness event we have been discussing crucial ethical choices around our protection of privacy and the need for important information and data to deal with COVID-19. These are not just questions around particular technologies such as blockchain, but about who we are as a people and our concern for each other as highly vulnerable human beings. Sensitivity to our social and cultural context is essential to making intelligent choices. The involvement of the whole range of stakeholders in such deliberations is essential.

Vicki Lemieux [00:16:08] Thank you, Michael. We have to leave it at that for now. And thank you very much. And to turn to our next lead witness, Rob Fraser. So, Rob, over to you to carry forward the conversation from where Michael left off.

Michael McDonald [00:16:25] Thanks, Vicki.

Robert Fraser

Robert Fraser [00:16:26] I doubt that I can carry on from where Michael left off, but I thought I'd give a slightly different perspective as I am not a researcher of privacy and security. Nonetheless, I find myself and my organization that I represent in the middle of a need to be very aware of these principles as we go forward and fully develop as a company. I will begin by giving a very brief introduction of who I represent; Molecular You Corporation is a young company out of Vancouver with offices in Edmonton and Toronto that has been developing leading technologies in identifying risk and ways to survey health over time, using a multiple multitude of technologies that just truly generate a fundamental, phenomenal amount of personal data, that make up a health profile of an individual.

We use this information to really help us understand health like we’ve never really been able to before. Dr. Lemieux had heard about Molecular You and the rich datasets we were gathering on individuals and recognized that we're dealing with private information that needed to be managed correctly. Putting this in context, many of our counterparts in this personal health space, like 23 and Me, had demonstrated that there's a lot of

---

value in human health data in that it could be sold to third parties for significant profit. In
the case of 23 and Me, this became their principal business model - selling the client
genetic data for their own profit and not that of the client and arguably without the
client’s informed consent.

Concerns are being raised around the world as to how we can use data like this to
advance our knowledge and benefit healthcare without violating the rights and privacy
of the data owner. We therefore engaged with Dr. Lemieux and her team to devise a
system to benefit from the knowledge that the data held without sacrificing the privacy
and control of the client. Our strategy is to give the control of data sharing to the
individual from where the data was gathered. And so not unlike the technology
proposed earlier by Nadia we went down the road of developing a blockchain solution
that would give individuals control of their data or self- sovereign identity and
management of their own data. We’ve been fortunate to get support to move this
forward through Canada’s Digital Technology Supercluster teamed up with Stone
Paper, Government of BC and UBC to develop an open source system with the goal of
making in broadly available to build a global ecosystem where data can be shared
under the control of the individual from where the data originated.

In this time of the COVID-19 pandemic, the approach that we are adopting has been
placed in a challenging situation where there is a global public need to access personal
data to understand the disease and its effects on its subjects so we can understand why
some people are at high risk to become sick or die whereas others are not affected at
all or suffer from mild cold-symptoms. Additionally, our core technology is ideally suited
to assessing risk of infected individuals, so we too have offered our expertise to help
fight COVID-19 and understand what health profiles evaluate risk for infected
individuals. Once we have this knowledge, we would have proposed to apply this to the
larger population with the idea that those at high risk need to remain in isolation
whereas those at low risk would be able to return to “normal” society. With the
continued studies of COVID-19 infected patients we have learned that infected people
may not be developing immunity to the virus. This challenges the concept of developing
immunity to COVID from a primary infection or a vaccine. MY’s primary technology of
risk assessment can be ideally suited to help decide who can and who should not be
reinstated in society. Recognizing the need to return to our normal lives at some level
and meet together to be productive as a society, we also need a way to properly
document or provide credentials that an individual is certified as a low or high risk for
stratification of the population and infected patients. We also need to be able to share
patient data across research groups to continue to unravel the mysteries of COVID-19.
So how do we accomplish this in a manner that still protects the identity of the individual, their own data, and allows them to get back into the workplace? Together with Vicki we’ve done a slight pivot in our development of our blockchain solution that would allow individuals to share their risk levels and or if we do are able to develop immunity or if somebody has vaccines, you can start to have these credentials that could be shared that are verifiable by the organization that issues them. With this in place we could start to get people back to work by incorporating this technology into our handheld devices. Simply by sharing the credential with a receiver (employer, border guard etc.) an individual would verify they are healthy enough or low risk enough to return back to work. I think this provides of a living example of how we can address both the societal issues of returning to function and maintain individual privacy. I say this in the context of our discussion today where we are still defining what privacy and data ownership means and discussing the best way to move forward as a society. Ultimately, it's up to the individual to make those decisions and whatever guides them to make those decisions; to share or not to share personal health data, to have tests that would show that there they're healthy enough to return to work or not and to share these credentials or not. The blockchain technology we are developing really will enable us to come to have our cake and eat it, too.

So I'll stop there being mindful of the time. I hope I have given a sufficient overview of how Molecular You is setting up these technologies into the work place and work practices, in the land of COVID, and on an ongoing basis as we start to enable more precise health management.

Vicki Lemieux [00:23:24] Thank you very much, Rob for your leadership in this this area. It's been an amazing opportunity to work with MolecularYou on developing some of this tech, these technologies.

Vicki Lemieux [00:23:58] And so my question to you, while other panelists are maybe thinking about questions they'd like to ask about the work that that we've been doing together and or about the work of MolecularYou is, you know, with some of these tests, not particularly the ones necessarily that MolecularYou is undertaking. I'm thinking more of the COVID-19 tests themselves. Some of the questions around, you know, the immunity antibodies. How can we be sure that even if we build privacy respecting technologies, that we're not creating this kind of structure for social discrimination? But I'm wondering if you. Do you have share a concern about that or do you have ideas on how we can make sure which test we can trust, for example?

Robert Fraser [00:25:06] Yeah. I think you raise some really good points.
Robert Fraser [00:25:09] And maybe the more sensitive one is this concept of those tests negative and those that test positive and who goes back to work and who does not and who's at high risk and who's not at high risk.

Robert Fraser [00:25:21] There's some efforts by the government right now to use genetic sequencing to identify who is predisposed to a COVID infection becoming a high risk of them.

Robert Fraser [00:25:37] And that one scares me a lot because genetics is one of those things that we're not very good at changing. And so I do worry about individuals being labeled for life as a high risk individual. I am also a little skeptical that genetic sequencing will actually determine if someone is at a high risk or not, it's very unlikely that individuals are uniquely genetically disposed in this manner. There may be very small numbers of them, but the majority of those people, the majority of the responses to infections are very complex.

Robert Fraser [00:26:24] What we know is that the predispositions to succumbing to the infection really come from comorbidities such as diabetes and cardiovascular disease [high blood pressure], so the better way to approach risk assessment is through MolecularYou’s technologies.

The development of vaccines may run into a few roadblocks on whether we do, in fact, have immunity against the virus. And therefore, if we would develop these so-called immunity passports, would that be of any value? If you're a high risk. And what does that risk mean? What's what's the full value of that? So there's still a lot of validation that's required. In our haste to get all of this done we are forcing answers maybe quicker than we have the proof.

Vicki Lemieux [00:28:25] Absolutely. Now we have a couple more minutes. And there is a question from Nadia here.

Vicki Lemieux [00:28:35] And if you care to respond, assuming you looked at the various varieties of blockchain DLT available, which blockchain platform did you select.

Robert Fraser [00:28:48] I am a novice in blockchain which is why I've teamed up with Vicki to help us navigate through the various technologies/ platforms available. What I do know is that we have gone with a hyper ledger platform. And Vicki, if you want to expand on that, much more capable than I am in discussing the technology of the blockchain.
Robert Fraser [00:29:14] Nadia, I'd be very interested in discussing the reasons for selecting this solution with you further as long as I have someone more technical to support the discussion. As I understand the real advantage that we've identified with the Hyperledger Indy is the ability to share credentials, whether it be in the form of data or the form of zero knowledge credentials, it fits nicely with what we're trying to accomplish.

Vicki Lemieux [00:29:44] So, you know, Rob has done an amazing job of learning about blockchain tech, which I think comes back to a point Michael made just before you spoke. Rob, that, you know, we need to bring people with diverse backgrounds into dialog. And so as a bioethicist, he's not a technological expert. And you certainly didn't enter the discussion, you know, with deep knowledge of blockchain. But I've heard you on many occasions speak very eloquently on the advantages of blockchain. You know, now, over the time that we've been working, So, likewise, I didn't enter into the collaboration with any background knowledge in healthcare or omic medicine. And I have learned; I would not consider myself any kind of an expert and would do a much poorer job of answering questions in this area than you have in answering questions on blockchain. So I think that there's much to be learned by this multi-disciplinary conversation and that needs to take place. And I just you know, rather than go into detail about the specifics of Hyperledger Indy, which is a self-sovereign identity type of blockchain solution, maybe, you know, if you could just reflect a little bit on the learning process and you know, how you've obviously been able to grasp this technology and what you think would be the foundation needed to do a broader education around perhaps some of the range of technologies that could be useful here. Any thoughts on that before we wrap up?

Robert Fraser [00:31:36] Well, I think one of the key strengths of the blockchain itself is that you have this immutable information. The technology we've adopted also has advantages from a security perspective, in that we can we share the credential rather than a big block of data.

In fact, the access is a link to the information securely housed in the cloud. Use of a linking system lends itself to some interesting interoperability possibilities that we're also working hard to include in our development roadmap. As I mentioned earlier, one of the biggest keys is that researchers need the data that Molecular You and others are generating for new learnings and do a better job developing new medicines and managing patients. The architecture we are developing allows our clients to decide if they want to share their data and if so do they want to profit from it. They interact with the interested third party in a completely anonymous fashion. Any transactions would be directly between the anonymized client and the interested third party. The other
application for a use case we are interested in developing involves sharing verifiable credentials with a third party, which we view as vital to the COVID situation today as mentioned earlier. I like the analogy of going into a bar and wanting to have a drink and being asked for evidence of legal age. You give your driver's license along with your photo I.D., your home address, your detailed birth date, your full name, and driver’s license number. None of this is needed to drink beer. Wouldn't it be far better to share verifiable credential issued by the same source that clearly states “I'm old enough to drink”?

I would like to add too that as we move forward we are very excited about the open source nature of the platform we are developing. We recognize that a network like the ecosystem we want to grow will expand faster and broader with less technical and financial barriers, not unlike the way the world wide web expanded exponentially.

Vicki Lemieux [00:35:00] Thank you very much, Rob, for really digging down into some of the technologies which we really haven't discussed in as much depth. That's right. And to carry on that conversation, Michael Cholod, who has a lot of depth in this technology as well. So, Michael, over to you.

Michael Cholod

Michael Cholod [00:35:23] ...Good afternoon, everybody. I hope you can see me. It is a beautiful sunny Vancouver afternoon. I want to thank you for the opportunity to give a statement. I must say that I'm deeply honored also to be, I think, the first non-PhD on this call. So it's time to dumb it down a little bit. I want to maybe put a little bit of context behind some of the different conversations we've had today and maybe get people thinking in a different manner. I think this issue that we're talking about right now is something that we are not actually really prepared to properly address right now. I would say, in fact, that we are even having such an important discussion at a time of pandemic when we've got governments and industry running around all over the place, frantically trying to put out fires about personal protective equipment, vaccines, testing, all of this stuff. That to me is an indication that we are not really ready, and neither are our governments ready to have a fundamental base level discussion about the power that we give to governments and or companies by allowing something like contact tracing at this moment.

I'm not saying that contact tracing is not a valid technology for limiting the spread of a pandemic disease. But I think the foundational technology and the foundational research behind what effects this technology would have and how to keep our data secure and private are not top of mind. So we're not going to be able to have a rational
discussion when it's kind of an afterthought. Everybody is focusing on let's just use technology to solve and flatten the curve and get us all back to work as fast as possible. One of the things that has been kind of an undercurrent in this whole discussion is the idea of privacy. Privacy is, in effect, a subjective reality because each of us has a different view of what privacy means. And so trying to find out how you have a one size fits all solution gets you into difficulties. I have been working on this idea of using blockchain based technology like distributed ledger and mesh networking to try to solve the problems of social media. Solving social media’s problem has become a self-sovereign identity problem. I would like to allude to some of the stuff that's already been presented. Right.

So one of the things, as Robert just said, as far as medical research comes into play, blockchain technology is a very valid solution, especially when you're dealing with sensitive information like patient health information. However, I suggest that the ultimate application of blockchain technology to something like medical records or something like contact tracing is self-sovereign identity. A true self-sovereign identity, is the most base level application of any kind of blockchain technology by taking it down to the individual level. Let's not forget that The WHO has called COVID-19 an infodemic and I think we need to keep in mind that that is essentially the bigger problem we have right now. This is not a moral or an ethical problem, it's an architectural problem.

We now exist in a world where the centralized structure of the Internet, based on honey pots of personal data, our personal data that is stored in databases near the services that are being provided. Our data is stored in walled gardens owned by governments or corporations. This is what Yann indicated earlier was a privacy paradox, because we're trying to solve the problem of individual privacy under the context of an individual who doesn't own any of their own data. This makes this a very difficult thing to solve a pandemic problem when we're all sitting around navel gazing, trying to figure out how to keep an individual users’ data secure. Whether it's health care data or contact tracing, whatever it may be, all of this data that we are talking about is created by the users. You, me, everybody on the streets, we create this data. So why are we not the final arbiter of how our data is used? And I think that's a very fundamental problem. We've architected the Internet as a centralized service because at the time we built it, we didn't have powerful enough computers. We didn't have fast enough connections. We needed to have it centralized so that we could get a service quickly. We no longer have that limitation anymore.

We all carry a supercomputer in our pocket. So there's no longer any reason for us to centralize the Internet around the service. It could be centralized around people. We need to stop thinking about how we adapt privacy and security to existing technologies
and start looking at new technologies like blockchain, distributed ledger, self-sovereign identity, things like this as the foundation for a new Internet. A new Internet based on users controlling their own data and access to services rather than a centralized control at a government or corporate level. If we do that, we solve Yann's paradox. Minister Murray alluded at the very beginning that this crisis gives us an opportunity to rethink how we do things.

So rethinking how we fundamentally structure the way we communicate is the real opportunity that we have right now. She also mentioned the strength of privacy in Germany. Right. I spent three years in Europe trying to sell software to the Germans, and they would sue you if you made a cold call to them. They're very paranoid about their privacy and data collection, because this is what their past has proven. What we've got to do is start thinking about how we solve a lot of these problems at an architectural level. We know if we had something like a self-sovereign solution where Holly and her group at the Provincial Health Authority could publish a study saying they were requesting information from people who had medical information from people who have had a melanoma. I've had a melanoma. I could volunteer that information with implied consent and there would be no more problems.

Dr. Alessi mentioned this problem of consent. But if we had if we all truly had a self-sovereign identity solution where we felt confident in some container or APP where we could put all of our banking and our personal information, then we could share it with anybody that we wanted to. It would get rid of the honey pots because the hackers are not going to go after an individual user just to grab one person’s identity. What we need to focus on, as Nadia mentioned, is blockchain. But we need to focus on its best application, which is self-sovereign identity as the silver bullet for all the problems ahead of us right now. For now, we cannot use contract tracing Apps I'm going to call that out right here. I think it's a clear violation of civil liberties. And no matter what sunset clauses are in place, we can't trust them. I don't think we can, especially some governments. to me, the better ideas for us to prepare for the next pandemic, because there is going to be one, and decide how we can safely implement things like contact tracing without requesting or requiring people to give up their civil liberties. That's my intro. Happy to take any questions if anybody's got them.

Vicki Lemieux [00:44:03] That's fantastic. Thank you, Michael. It generated a lot of discussion and I don't know if you'll have time to respond to everything but there are questions in the Zoom chat as well. So please feel free to respond to any of those.

Michael Cholod [00:44:20] Right. You are assuming a degree of connectivity that does not reflect our whole society. Continually marginalized groups in our society. The
Downtown Eastside of those living on remote reserves. Absolutely. I absolutely agree with that. It was mentioned earlier that we've got some people, elderly folks, for example, people who may have dementia or things and cannot use technology. Self-sovereign identity isn't going to be a silver bullet for everything but I think it is a better base to build upon. We need to build a solution that protects as many individual users as possible and self-sovereign identity can do that.

Michael Cholod [00:44:57] So I hope that answered that.

Michael Cholod [00:45:02] Let's just see here what we got over in the queue.

Vicki Lemieux [00:45:05] Yeah, there's a question about just clearing up, which you may not be able to answer, but seems to be a misunderstanding about the contact tracing. So this person is pointing out that the contact tracing apps have been strongly focused on privacy from the beginning. That is why they are exchanging really long numbers, via Bluetooth.

Michael Cholod [00:45:33] There's lots of information out there on the contact tracing and how these apps work but the number one thing I keep seeing is that in order for them to be completely accurate and to actually work really well, the entire population has to be on them. We all have to be tracked. It not just important that marginal groups have access to contact tracing, we all have to do this. But the governments are saying do it in a voluntary way. So the know right then and there, you've got a paradox, because if you're going to ask people to volunteer, the people that don't volunteer are walking disease factories. And the people that do volunteer are being led into a path where now they're being tracked 24/7 for the rest of their lives.

Vicki Lemieux [00:46:20] And people could start to respond to that by saying "What, you're not volunteering?" There could be sort of like a social shaming angle.

Vicki Lemieux [00:46:32] I think there are many, many aspects of this to be considered. So, Michael, thank you so much.


---

30 Suggested Reading

Jesse McKee

Jesse McKee [00:46:51] Hi, Victoria. Thanks for looping me into the call today. Good afternoon and evening to all from the unceded, traditional and ancestral territories of the Musqueam, Squamish and Tsleil-Waututh First Nations, also known as Vancouver. I'll just preface my words with a little bit of my own background, education and training which is in political science, critical theory, visual art design and curatorial studies. I've worked mostly as a curator of contemporary art and design in places like the Barbican, the Banff Center, and now as a leader of a non-profit in Vancouver called 221A. We work with artists and designers to research and develop social, cultural and ecological infrastructure.

Victoria and I know each other from her work on the blockchain research cluster at UBC, and she's sitting as an advisor on my non-profit's three-year research initiative funded by the Canada Council for the Arts, which we're calling Blockchains & Cultural Padlocks. Through this project we're looking at the ways blockchain can be used to “re-common” land, objects and data. I think that's a good place to start to consider: what are our cultural padlocks that keep us from accessing the ways of operating we so desperately need right now in the COVID-19 pandemic?

And I'm with Michael in the previous statement; I don't think we're going to get it right for this pandemic, but I think these conversations are going to get us somewhere for the next one. So, while working through the pandemic, I've been using my own cultural analysis lenses and acting like a sponge in some strange and darker corners of the Internet. Or maybe I'm just getting outside of my own filter and content bubbles, which is always good to do, despite what you might find. Admittedly, the design and critical theory bubble is the one which I'm a fully-fledged member of. I've been engaged with different forms of debate and publishing, and I do want to give a shout-out thanks to an online community that I'm a part of that has helped focus and aggregate some of this content into more coherent data, and that is the New Models community. Check them out at newmodels.io

New Models acts as a human-powered aggregator for news and analysis on media, tech, politics, culture, health, ecology and economics. And, it's


paired with a couple of podcast streams and a Discord for community building and feedback. They're also a contributor to our blockchain research at 221A.

I’m immunocompromised and I’ve been in total isolation since early March. I haven't gone outside, except for my balcony, for well over a month now, because so few people are wearing face coverings and masks in my neighbourhood, nor do they really understand what a distance of two metres is without a hard visual guide. So it's pretty bloody dangerous for me outside right now. And that's because we cannot get on a shared narrative together.

I just want to echo Michael's notes about the infodemic. The central narrative around COVID is a huge challenge. And someone that I've been reading lately is Venkatesh Rao, of Ribbon Farm blog, Breaking Smart podcast, as well as The Art of the Gig blog. He notes in his writings recently that during major moments of human catastrophe, we lose the plot of a common narrative and just feed on raw data, facts and news. He says that only in hindsight can we really spin new narratives that people can get on board with and reinforce with their own choices. We really should be looking at those who can help us reestablish narratives, because the neoliberal politics and economics we have now are not really sufficient enough to lead us during a crisis.

I don't like how China and Korea have been deemed draconian for the way they approached the pandemic with digital information and contact tracing. They clearly had the political and organizational prowess to implement their modeling and tracing in ways that seemed like they were about a decade ahead from Europe and North America's abilities. In the global former West where we are, liberal democracies have done some good in this pandemic, but it feels like the bare minimum. The way we operate politically and ideologically has also done us a disservice in the broader scope of this crisis. We’re in this infodemic, as Michael has said, and it is only made more severe because of the way our liberal democracies approach and fail to understand tech.

Benjamin Bratton, a crucial leader on the thinking behind city-wide and planetary-scale computation (who is at University of California, San Diego and the Strelka Institute, Moscow), recently published a text that was called “18 Lessons of Quarantine Urbanism.” In it, he says that the epidemiological view of society is changing, and that it's a mistake to reflexively interpret all forms of sensing and modeling as surveillance, and all forms of active digital governance as social control. We need a different and more nuanced vocabulary. In actuality, this pandemic is more of a major reawakening of what Bratton has been calling “revenge of the real” or “reality catches up mode.”

during this pandemic, we see all the blindspots of the neoliberal ideology now with spotlights on them. We see vast equity gaps, weak social and medical infrastructure, fractured social narratives, disastrous and divisive social media architecture and lapses in research and progress at the policy level around the digital realm from our regulatory bodies. This all combines to make COVID-19 the largest experiment in comparative governance. The virus is but a control variable and the results speak for themselves, as Bratton has said.

And then I look to a text published early on in the pandemic by the philosopher Slavoj Žižek. To be honest, I’m not usually a fan of his bombastic tone, but he covers so much ground at a high resolution and reasonably well in this text, which is calling for a return to the commons, or communal solidarity, and asks: how can the virus bridge us to a more socially cohesive and coherent planet, and map the world that we can grow into? His text is aptly titled “Monitor and Punish? Yes, Please!” He goes back to Kübler-Ross’ five stages of accepting loss and death. He spells out our own misgivings about digital tracing and modeling and the growing threat of digital control over our lives. He states, “first, we tend to deny it (it’s an exaggeration, a Leftist paranoia, no agency can control our daily activity…), then we explode in anger (at big companies and secret state agencies who know us better than we know ourselves and use this knowledge to control and manipulate us), which is followed by bargaining (authorities have the right to search for terrorists, but not to infringe upon our privacy…), depression (it’s too late, our privacy is lost, the time of personal freedoms is over), and, finally, acceptance: digital control is a threat to our freedom; we should make the public aware of all its dimensions and engage in fighting it!”

Going back to Venkatesh Rao, he seconds this is in his text Murder on the History Express, recognizing a swift death of the industrial era with the arrival of COVID as we’re being pushed into a “nascent world already eaten by insufficient software.” Zoom is one of the consumer examples, the platform we are using today. But a government intellectually and materially unprepared to digitally model and sense its citizens as a matter of public health and social order is far scarier than having your meeting interrupted.


I'm looking forward to a new book called *Quarantine Architecture*[^36] that should be out soon by the American architect and writer Jeff Manaugh and his partner Nicola Twilley. Jeff leads the blog BLDGBLOG, and Nicola is a writer from The New Yorker. They're about to finish and publish a history of quarantine architecture while in quarantine. But this was something that was started well before COVID arrived. It is important to think in terms of the historical layering that pandemics bring, and they want us to note how temporary measures put in place to meet the crisis tend to stick around as defaults in the future, even after the virus has passed. They cite a couple of examples, and a very concrete one that stuck in my mind is the current-day border between Egypt and Sudan[^37], and how this was drawn from the historic quarantine checkpoints between the territories. What we can use this knowledge for now is to pay attention to the ways digital platform design and protocols are being amended to meet the needs of our quarantine, and how this could set into stone the next layer of the web, instead of our dreams of decentralization.

So to think of our digital architecture going forward, consider this quote by them on the history of quarantine architecture: “You can't build an entire separate infrastructure to sit there empty in case of a pandemic. But you can build a shadow pandemic architecture into your existing architecture by thinking through your needs. Can you mandate that these large structures are transformable?” That's a good question for us to consider. These writers may be thinking about a conference center, and how the conference centers can now be designed as adaptable architectures that could rapidly be transitioned into quarantine centers for future pandemics.

Of course, we did do that already, but they’re not great. It was not thought of at the original design tables. Everything has been jerry-rigged into the existing static infrastructure. So what can we do in our digital architecture right now that would allow us to transition over to these moments of crisis, when there is an immediate need for the technology to enact a kind of tracing and system to alert the public and regulators, and then to switch it back or turn it off when the threat has passed? I'd be curious to know if there’s anybody who knows of anything like this underway.

Where it gets hard for us who are leading these conversations and investigations is toeing the line of questioning the policy and the policy makers, providing comprehensive


resources, and driving the conversation towards better outcomes. Hello, 221A’s model! How can we do this without inflaming radicals on either end of the spectrum? That's the challenge. And what we're seeing with COVID is there is this horseshoe effect\(^\text{38}\) of the political spectrum, which is bringing the far-left kind of biopolitics-or-bust Agamben readers alongside far-right positions. We've already seen the danger of such a turn in some ways with the Gilets Jaunès movement in France, which disabled Paris every weekend of 2019 and the beginnings of this year. It's not quite the same configuration of groups that we're looking at with COVID, but the same horseshoe effect has taken place. In North America it is the radical ends of the spectrum who've been disqualified from neoliberalism’s economy and culture, and they're now angry, not listening to expertise and congregating en-masse together.

So we're seeing COVID inflame and unite previously far-divided factions. I'd say our situation locally is also at stake where groups of these protesters--who may be vegan, pro-organic, non-GMO anti-vaxxers--will stand beside libertarians and white supremacists. They collectively support each other in this instance when they think the lockdown and any modeling and sensing measures are an affront to their personal liberties. They will violently oppose any state action to deal with a pandemic. Some of you might be asking, why would white supremacists be involved in protesting public health responses to a pandemic? Well, they know that this virus is killing racialized people in far greater numbers than whites. The US intelligence community found instances of white power groups trying to spread COVID into racialized communities as early as the first weeks of February. This is a brutal reminder that income is the deciding factor as a measure of health and stamina under neoliberalism, especially in North America. So, previously opposing political factions are mutating together into a new political force, and they're using COVID to accelerate their hold on power with a growing base.

We don't want COVID to fuel this kind of political momentum in Canada, in Europe or in the US. In the US it may already be too late as these groups have financing from people connected to Trump's cabinet\(^\text{39}\) already, which is part of that administration’s nonlinear info-war against its own citizens. This new kind of amorphous and reactionary alliance kind of politics is so hard to counter, and instead it just becomes the new popular opinion driving policy. We need a broader spectrum of expertise working on these kinds of projects that model and sense our society, in order to develop the hard mechanics and ethics of our rapidly transforming world.


I'm looking at a future, likely from a younger generation’s perspective, that is seeing government and platforms co-evolve in ways that we haven't before. And so we need to stay close to all parties in the public sector and the private sector. We need to stay sharply critical and vocal, and we need to share as much knowledge right now as possible. Thanks again for inviting me to do just that.

Vicki Lemieux [00:59:08] That's fantastic. Thanks, Jesse. You know, I always find your ideas really stimulating and really forward-thinking. There's a lot we can go into but we're coming up against the time though. So I think we might just leave it at that. And unless there's something pressing, you want to address in the Chat or the Q&A. But I'll invite people to review the bibliography you've put together to delve more deeply into some of that, the rich ideas that you shared with us. I particularly have been inspired by the idea of governments and platforms co-evolving which you've mentioned before. And so I think that there's a lot to be explored in that regard.

Vicki Lemieux [01:00:06] OK. All right. Thank you so much. So, Steve, I think that it's over to you now.

Vicki Lemieux [01:00:13] I'm going to pass the baton and invite you to carry forward the conversation. Thanks again, Jesse. Over to you, Steve.

Steve Magennis

Steve Magennis [01:00:22] First of all, thank you for having me here today. This is the first event of this type I’ve attended and it's been really great. There has been a lot of good conversation on the topics I think everybody is struggling with. On the one hand, I think this validates the areas of concern that most people who are in the space have, but also provides a lot more depth than any one individual can bring to a topic. So thank you.

I'm not sure I can bring a lot of new insight into this conversation, but what I can do is talk about this space from my perspective. The way I’d like to start is to think about what happens if we are successful in using data to mitigate the impacts of COVID-19. If we are successful, then what we will have effectively done is deploy an inter-connected technology, and social infrastructure on a national or even global scale designed to gather information about us as individuals and about our health. Once the initial crisis has abated, there will be ongoing temptation to continue to leverage that now-functioning capability and to follow the precedents that we set - all under the rubric of social good.

I'm not saying that this will be a smokescreen. I think people will be very in earnest in pursuing this ideal. But the machinery will be built up and people will want to continue to
use it. So, the question I have is what sort of guardrails do there need to be to keep things in check?

I frequently espouse the notion that there are some problems you can solve and some you can only manage. I think when we talk about security and privacy in particular, these are problems you can only manage. Security is a never-ending arms race. We'll come up with some great, secure cryptography and someone will come up with quantum computing to break that, and so on and so forth. Where there's a will, people will bend what they have to their purpose. Some intents will be nefarious, some less so, but it's something that we need to look at in terms of how to manage it.

When I think about guardrails, I think about four interrelated vectors. The first one is technology, and right now there's some really, really incredible technology coming out that I think helps shift the balance away from centralized top-down control to more individual control. Some of these technologies you've heard a lot about today: self-sovereign identity, cryptography, verifiable credentials. It's a sort of tool bag of technologies that allow you to shift things a little bit more towards the individual and individual privacy, which I think is a really good thing. Quite frankly, I think it's desperately needed now. The new technology enables us to solve classes of problems that couldn't readily be solved before. For example, there has been a lot of conversation about institutions and organizations being required to delete data once the data has been used for a specific purpose. There has been a lot of discussion about whether this is good or bad, or even possible. Well, now we've got another way of looking at this problem. We can now talk about having data that is encrypted and controlled by an individual or proxy of an individual so that the data doesn't necessarily have to be deleted, but can be unlocked and repurposed given the right situation.

This is just one example of some of the things that technology can drive, but it can't do it alone. So we also look at governance and laws to play a role. GDPR is probably the most well-known example. I was just on a call a few minutes ago with the Linux Foundation about something called Trust over IP, which is really a governance stack surrounding decentralized technology. When building and deploying these kinds of systems that are privacy preserving or decentralized, they are not a free for all, but rather governed by rules and conditions that people jointly agree to. Governance can be codified in law or it can be a contractual obligation, but the idea is that people who participate in these governance organizations set themselves apart as saying, “we've taken it upon ourselves to adhere to certain rules and regulations.” The consumer then, can have an elevated degree of trust that the ecosystem will operate according to a known set of standards.
Another guardrail vector I've been thinking a lot about lately is the notion of social norms and risk. This is the area where I think the most work needs to happen. Over generations we've become pretty good at managing personal risk and privacy when we're dealing pieces of paper and one on one interactions. We've developed an innate sense, for example, of who we can show our driver's license to and still be pretty safe. With the technology that we wield today and the massive interconnectedness of it all, the rules have changed. It's a lot easier for information to get out into the wild and stay out, and thereby lose control over it.

How should somebody respond once they know personal information about somebody else? For example, if I'm an employer, at any given time I assume there will be some number of people who are sick but still come to work. But I accept that, as 'acceptable risk.' I know that maybe somebody else is going to get sick through contact and because of that I may lose more productivity and so forth. That scenario is just something I've gotten comfortable with. What happens then if somehow, I can be certain down to the individual, who is going to be sick that day? How am I going to respond to that new information available to me? I think the natural tendency is that I, as the employer, will want to somehow use that information to reduce my risk. So perhaps we need to re-evaluating our social contract. When is it acceptable for someone to be restricted from working or restricted from flying, perhaps restricted from all sorts of other things? Just because I know more information about someone, can I use the information in a way that shifts risk from me to you? I think these are social questions we have to deal with.

On the flip side. How do I as an individual respond to other people knowing information about me? Social media is a perfect example. A generation ago, the notion of letting the public know what you had for lunch, where you're going, seeing pictures of your kids at home and all that kind of stuff would be abhorrent. We do that now with abandon because socially, we've become comfortable with it.

If you think about privacy in terms of personal risk, it can be thought of as a mental calculation of the chance that something may or may not happen to oneself. If I tell somebody something in confidence, how likely is it that it will come back and cause me a problem, or how likely is it that it will come back and benefit me at some future point? These are types of formulas that we have to reevaluate in a highly connected world.

Technology is great, laws and governance are great, social norms are great They each contribute, but they don't solve the entire problem. What is the backstop if all of these fail? What sort of recourse is available? If information gets out that could ruin my career, or ruin my life, that's a very dangerous thing as opposed to information that might just
be inconvenient or embarrassing. Are there meaningful ways to compensate somebody for damages caused by exposure of personal information? In the past, there was a lot of friction to information movement. I maybe had to have a piece of paper or had to tell somebody something person to person, and that person if they want to disseminate the information, had few channels at their disposal. Most of them costly or complex. Now, it's very, very easy for information to flow quickly and get out of control just as quickly. Once information is in the wild, what does it mean to compensate somebody? Conversely, should we really be as punitive as a society just because we now have access to information we were never able to access before? Again, these questions call for us to reevaluate our social contract.

From a societal perspective and from a technology perspective, I think everything is generally moving in the right direction and in good faith. A lot of smart, committed people are working to make this happen. Many feel strongly that privacy needs to be rebalanced and thought about in new ways. The landscape though, is moving really quickly, and the COVID pandemic has supercharged everything. It's forcing us to evaluate technology and re-evaluate social underpinnings at a breakneck pace that would normally take us a long time to internalize. It is forcing us to look at these things and make tough decisions very quickly.

I believe the natural consequence of this is that we’re not going to get it right the first time. Even if we had all the time in the world, I don’t think we would ever get it perfect. That simply means going forward, we will need to continue to work along all four vectors to make the guardrails work the way they should.

I think we all want to have privacy, whatever privacy means for us now, and we also want to have good data available to benefit society as a whole, and even to make sure that when we do a Google search, we get highly personalized ads. Along the way, we will need to reset our social contract.

Vicki Lemieux [01:11:10] Steve, thank you very much.

Vicki Lemieux [01:11:12] I think it's really important that you focused on this notion of reevaluating the social contract, because in a digital world it seems that, some of the basic elements of the social contract and it isn't even the digital world. I mean, I think that, you know, even before we could describe ourselves as living wholeheartedly in the digital moment that we are now, that the social contract has been under strain, thinking about some of the Edelman Trust survey results so that it's really important to raise that question. I raised a question on the chart, which you can choose to respond to. We've got a couple more minutes before we have to move on or you can you can elaborate on
it on some of the other points that you wanted to make. So I'll leave it to you to carry forward the discussion for the rest of your moment.

Steve Magennis [01:12:09] Let me address Michael's comment. I guess he's responding to your comment about the disparity between certain marginalized individuals and those who have authority. My perspective is that it's an unfortunate outcome of the human condition that there will be those that have authority and power and those who are marginalized.

Going back to my previous comment, I don't believe this is a problem that can be solved, only managed. I think we should have the conversation about whether we think the degree to which the marginalized or disproportionately disadvantaged needs to be shifted and find a way that we can help rebalance those things. I'd like to think that everybody can have a seat at the same table and have meaningful power and influence in society. But I think if history tells us one thing, is that's probably not going to happen. It's a matter of ebbs and flows and as a society we land where we land for all kinds of reasons.

Vicki Lemieux [01:13:19] Yeah, yeah, that's very true, and our social institutions, as much as our technologies, seem to have a great bearing on that algorithm. If we want to use that phrase. Thomas Piketty has as written a lot about social inequities and in terms of financial inequities and how they can rebound over time. So I think it's really important to think about the now. It's also to think about important to think about, you know, maybe how that aggregates over. Over time. There's another question on that. A couple more questions on the chat. And I think we've got maybe one more minute for your interventions if you want to respond to any of those. Well, I'm a treat.

Steve Magennis [01:14:04] I'm intrigued by the question: “Should the right to anonymity be part of a new social contract?” This is something I've given a lot of thought to. I think that the term anonymity is it's too blunt of an instrument. We all have stated personas that we put out into the world: your work persona, your persona with your spouse, your persona with friends and family. With each of those there is a certain amount, if you will, of anonymity that you present and insist upon. So as a blanket statement, should anonymity be part of a social contract? Absolutely. It has always been there and always should be. The question is more to what degree? In what context? Under the umbrella of anonymity a lot of really bad things have happened in this world. And frankly, under the under the banner of transparency and disclosure, lots of bad things have happened.

---

The way in which anonymity should be manifest is the subject of many ongoing conversations.

Vicki Lemieux [01:15:16] So thank you again, Steve. You know, again, another intervention of yours that has raised really important and deep questions for further explicit exploration, which, Paola, over to you now to carry the conversation forward from where Steve left off. Thank you so much.

Paola Ardiles

Paola Ardiles [01:15:56] First of all, I just want to say thank you so much for this invitation. It’s been a fascinating discussion. I can’t believe that I’ve actually been able to hold this whole thread. I think that it was really important for me because I feel that the best solutions really come from bringing people together that think differently. So I wanted to just applaud Victoria and Michelle and all the folks at UBC that have put this together, because I think that it’s really important to have these diverse voices and expertise. So I’m going to be speaking from my experience and I like to use this term called grounded expertise, which is really sort of like a combination of my lived experience as well as my policy and research work related to community engagement, because I think that it’s really led me to use an equity lens in relation to public health issues. So I’ll start there.

I’m a former refugee and I’m living here on unceded territories of the Coast Salish peoples. I am the co-founder of Bridge for Health, which is a network that is focused on health, equity and community participation in relation to health and well-being. And over the last five years, I’ve been co-designing community academic partnerships in my faculty position at Simon Fraser University, around building social innovation labs—the focus has been is really engaging students and community on solving complex problems related to public health issues in the local community of Surrey.

---


43 City of Surrey. (n.d.). [Surrey CityLab.](https://www.surrey.ca/community/28110.aspx)

44 Faculty of Health Sciences, Simon Fraser University. (n.d.). [Health Innovation at SFU.](https://www.sfu.ca/fhs/undergraduate/current/get-involved/health-innovation.html)
So I think I'm going to start by saying that this is a very important dialogue that's happening now during the pandemic because the time to engage the public is not after, it is now! And so I again, I really appreciate the opportunity. So a couple of things I wanted to say is that the I'm going to also be speaking from the my own perspective informed by being a part of marginalized and racialized communities. I really appreciate the comments that have come before that have touched upon that. When we think about engaging the public, we're always thinking about, why is there is such difficulties in engaging and building trust? And I think we need to recognize that there are deep historical roots, and that we need to be posing questions around the use of health technologies for public good. And is it for the good of all? We've already seen evidence that there is a higher impact on marginalized and racialized groups when it comes to COVID cases. I think that there's also evidence around differential impacts related to gender.

So I think one of the things I've really appreciated is the COVID it has brought to light some of the issues that we have around lack of data in relation to equity. Also it has also brought around a lot of conversations about how do we use equity informed and gender equity informed approaches to our responses at a government level. We've talked to a lot in this discussion today about how we all have different experiences, different knowledge bases, and that really shapes the way that we see, we define and we experience privacy and health technologies. I think that what is important from my perspective is really thinking about how people's lived experiences intersect with these concepts of privacy. And what I mean by that is that we all have different levels of trust in relation to government, to public and the private sector. And it all becomes enmeshed as we've talked about the complexity around privacy. I think that there are other things that we need to be considering, for example, language and cultural barriers that many marginalized and racialized communities face.

The language around ‘contract tracing’ and even ‘exposure’ can be very triggering, and I think that we need to be cognizant of what language we are using. I come from public health where we study a lot of the structural and social determinants of health. I would say particularly thinking about experiences of violence and discrimination and how that impacts the way we even talk about data and public health surveillance. Because building safety can be a very loaded concept for those that have faced historical trauma and colonization. So, we have to think about this as we're building this trajectory towards better governance and privacy-we need to be thinking about it within the lessons that we continue to learn around Indigenous Peoples and the consequences faced by residential schools, for example. We need to be thinking about it in the context of migrants who come to Canada from situations of extreme violence and often state violence. What I wanted to pose is that we can't think of people's lived experiences as
something separate to the way that they see themselves in this high tech world and thinking about privacy, because all of those factors, language barriers, literacy rates, whether people are housed or not housed, gender, all of those things have a cumulative effect.

So I think it's really important to be thinking about what are the unique conditions that communities are facing. One of the examples I've been thinking about is this whole concept around the immunity passports, and how that concept is making a lot of people very nervous, especially if you have been part of a community faced with increased policing or state violence, also increased incarceration in some in some countries. I think we need to be naming these things, naming that there is racism in the system, there is racism in the health care system, there is discrimination. Also, not everybody has equal access to the health technologies. Speakers before mentioned the issue around access to smartphones. In relation to access to Wi-Fi and Internet connection, I've been thinking a lot about people in remote and rural areas and also thinking about people that are living with cognitive impairments or physical disabilities. So I think that all of these things are really complex.

As we are building dialogue and public engagement around how do we build trust, how do we taking into consideration all of these factors are influencing our privacy concerns. My challenge is how do we start thinking about this from an equity lens or a just social justice framework where we can be thinking about building these technologies that are actually good for all and not just some. So, thinking about what are the impacts that we might be creating without even being aware or being conscious of it. I want to say that I think that this is an opportunity to re-imagine how we can build trust and design with an equity lens in mind. I think that achieving balance and transparency is something I've heard a lot in this conversation and for me it is really about advocating for meaningful participation into processes and policies. I think that it means that we as designers, researchers or government, need to be thinking about our own positions of power and privilege.

How we can best understand what the relationship is between the designers of these technologies and the users of the technology and thinking about our own assumptions and our own biases. Do people really have equal access to data? What about the levels of health literacy? How do we build privacy for the homeless communities? I think that there's a wide range of tools out there that we can use. You know, there's a lot of work around empathy and looking at human centered design approaches.45 There is also a

lot of work around participatory and equity approaches that we can use in design. So I think we need to be carefully considering how we use the spectrum of engagement and really bring people together on co-designing. I think it's going to help us definitely ensure that what we're creating is actually more relevant, but it's also going to be building trust. I think that it's really important to think about investing in public engagement as much as we're investing in I.T. infrastructure and systems. So I'll wrap up with this remark at the end that maybe it's time for us to start re-thinking the “how.”

How do we think about public engagement in relation to privacy without thinking that these marginalized populations are ‘hard to reach’, and shift towards a perspective where we are thinking about how do we best serve marginalized communities that are ‘hardly reached’, because I think that the efficacy and the speed of the uptake of any technology is going to be dependent on the levels of trust that we're building through our engagement processes. Thank you

Vicki Lemieux [01:25:42] Thanks so much, Paola. Really important observations there. So I don’t know if you want to respond to I posted a question on the chat.

Vicki Lemieux [01:25:56] If there are other questions that others have for Paola.

Paola Ardiles [01:25:56] I cannot see them yet. Would you mind just…if I have time to answer it? I'll try to answer one of them

Vicki Lemieux [01:25:56] Sure I'll just read out the question that I posted for you. So you mentioned human centered design and empathetic design as being a way to design technologies upstream that take into consideration the unique communities. And there are the hardly reached. I wonder though, it's sometimes very difficult to predict unintended consequences even for those communities themselves. And, I'm just wondering if you've come across in your travels any techniques or strategies for how we can get people to think a little bit outside the box about potential unintended consequences. This is something that's always really difficult, I think.

Paola Ardiles [01:26:59] Well, I think that what you're doing here is really aligned to my philosophy on this as I really do believe in co-design and meaningful participation of as many diverse voices as possible. So I think, there's no fool proof mechanism or process where we're going to understand all of the unintended consequences that may come.

---


But I think that by meaningfully engaging the community that we're trying to serve in a way that is real and not just like an afterthought. I think it's really the way forward.

Vicki Lemieux [01:27:33] Yeah, yeah, absolutely. The key point being not an afterthought and difficult to make it like everything's almost an afterthought when you're dealing with everything at the speed of a pandemic.

Paola Ardiles [01:27:46] That's right. But now we really do have an opportunity. I think that that's why I'm excited about this, is that we actually have a real opportunity to re-imagine what that future is going to look like with all of the knowledge base and all of the experiences that we've acquired and shared.

Vicki Lemieux [01:28:01] Yeah, absolutely. And as you say, so many diverse voices. So thank you for adding your own to all of the diverse voices. And so at this point, I'd like to pass the baton again to Nora.

Nora Weber

Nora Weber [00:00:16]: Thank you to all the participants. I've been so impressed with the diversity of opinion and background, and it will inform me about what I do. Just a little bit about me: I've worked at the U.N. for an NGO and in that role I worked with Advocates for African Food Security, an NGO formed by African women who were there with other NGOs who formed their own to bring attention that if you fund women in development, it's much more sustainable, which is now more much more broadly known than it was then. I have also collaborated with the Vienna Academy for the Study of the Future, which was run by royalty, but included physicists, futurists, and environmentalists. I also have a background in radio and television and, where television is concerned, it's run the gamut from current affairs to television drama. So I am very much of a generalist. I've had 30 years of running my own communications company specializing in culture, environment and social justice, and all of that informs what I have to say.

I wanted to really thank you for having Ann Cavoukian start us off because she talked about a principles-based approach. Unless we do that, as Paola has also pointed out, the dominant voice wins. So, principles are a really important part of solutions. I often think that some of those principles are ones that we try to teach our children. I used to tell my son that trust was not something given, it is earned and that it is earned through our deeds, not just what we say. Part of a principles-based approach is also respectful listening and reciprocity because, without those things, we tend to exclude (or assume) rather than include. The greater good can often be read or translated as the dominant
good. And that's something that Paula alluded to as well. I'm not a technical person. In fact, I'm a techno idiot. But I am a communicator.

Nora Weber [00:02:35] In order for something like an app or a way of contact people to be taken up, it requires public trust and it needs to be communicated in a way that people see their own good and the greater good at the same time. So that's the part of this that I will address and then talk about the privacy issue from a principles base. Justice is one of those overarching principles. And in order to be just, we have to include the most vulnerable – and not just include them as an afterthought, because that's typically whitewashing, literally and otherwise. It's important to really listen to what works for them. I'll give you an example. I consider myself an ally and it's a constant learning position to be in.

Nora Weber [00:03:32] I remember speaking to an elder and asking her if service was the most important attribute for Chiefs and Elders.

Nora Weber [00:03:44] And she said, no, that was second. The first was listening. Even in style of listening, we tend to come from a dominant culture, with a few exceptions. We tend to be schooled in debate and persuasion. My field is full of persuasion. If we instead talk about inclusion, diverse points of view, then we get closer to stakeholder relations in a way that, for example, brings us back to effective contact tracing. People will trust us and trust each other to share information where it's needed with limitations. There is often, within the minority voice, very important information that will apply to all of us. (For example) If you can get someone in the Downtown Eastside to be okay with contact tracing to effectively use it, you’re more likely to control the pandemic among the most disadvantaged.

Nora Weber [00:05:00] If you can have people who have language issues in this culture and communicate through their language and their cultural lens override privacy to download a contract tracing app, then you reach much further (toward sufficient uptake).

Systems theory says that the maximum moment of chaos is also the maximum potential for change. I think we can agree that we’re there right now where this pandemic is concerned. So I would hope – and it's certainly become clear with all the participants – that the aim is to come forward toward a larger, more inclusive solution.

Nora Weber [00:05:45] I remember someone saying that the internet has democratized knowledge. You can find anything online, but it's also been used for nefarious purposes, hacking being one of those, and misinforming being another. Who's in charge of the information? Is it a corporate agenda? Is it a control agenda? All of those things are
important. The internet has certainly been used to alter reality through fake news. And one has to only look south of the border to see that some people have a completely different view of what democracy is and what greater good is. So we need to be careful about unintended consequences (and interpretations of motive).

Warren Buffett said only when the tide is out, do we see who is swimming naked. Of course, he was applying that to economics, but you can certainly apply it to anything from effective information gathering to securing privacy. Privacy (in a democracy) requires trustworthiness as government entities or health policy officials.

Once this pandemic is over, do we own up to our mistakes? Does our transparency include discussing what did work or what didn't work? How did we get to a more inclusive solution? What are the lessons learned? If we take a solution orientation rather than a problem orientation, what social agreements do we need? We need to include minorities to get to the greater good – that greater good being inclusive rather than exclusive. Do we look at outcomes? What outcomes do we want? Have we clearly stated what those outcomes are that we're aiming towards? And have we shared that with the public?

Nora Weber [00:07:48] The other thing, when it comes to sharing health information, especially with something like this pandemic, there should be a lot of interdisciplinary sharing. For example, there has been a conversation on the Internet about the pandemic being a result of our environment being overrun, with the virus and wildlife coming closer in contact with us. (How can the data gathered about the pandemic be used to further inform the research on the intersection of new diseases and deteriorating environment?)

Nora Weber [00:08:17] While some of the data gathered perhaps needs to be anonymized. However, instead of everything being anonymized, can critical and relevant information be shared within eco-districts like Indigenous communities or refugee communities? We do know that some communities will be more vulnerable than others, whether because of vulnerabilities to health conditions or because of economics or because lack of information or lack of accessibility to Internet. (For example, unlike the US, Canada does not include race in a lot of data gathering)

This is more fodder for discussion than actual solutions or particular stances, but I think that it's important to consider these issues. While we do have some Europeans on this call but, to my knowledge, we don't have Africans or residents in Asia, so we're missing their perspective for a world-embracing solution. If you're in Africa and you live in the city versus the tribal societies in the country, these challenges affect the effectiveness of
information gathering. I would hope that we're looking for global best practices in all of this.

Another consideration is style of communication. For example, I've learned from the Indigenous community that speaking quickly is not necessarily the style given to other cultures. For many, it's listening and speaking little, then speaking as sacred contract where listening is a kind of sacred witnessing. Within that context it's important to take the time to speak truth, from the heart, and with the service of the community in mind.

It's important to consider outcome harvesting in the policy-oriented phrase.

Nora Weber [00:10:49] Thank you very much. And I do want to say as well that I'm on Katzie territory, and until relatively recently, about 20 years ago, they were told they were extinct. So those are the kind of factors that come into this as a subtext. Thank you.

Vicki Lemieux [00:11:07] Thank you, Nora. That's a great reminder point to end your intervention on.

Vicki Lemieux [00:11:17] There's a couple of comments and questions on the chat. And I just invite you to carry forward your discussion by reflecting on those questions or if there's anything else that you would like to reflect on from previous questions.

Nora Weber [00:11:37] Well, I'd like to answer your question on the concept of eco districts and its definition. I work in environmental circles as well, and that concept has been used for city environmental development within Portland specifically, so I've borrowed that phrase to think in terms of Indigenous communities. For example, coastal Indigenous communities are very different than plains Indigenous communities in their historic development and in what they prioritize environmentally and so on. And so the data, while it needs to be anonymized to some degree, one would want, for example, those communities – and Paola could speak to this better than I could – those communities that could benefit from the information to use it for their own purposes, like Indigenous communities or refugee communities. I think, from a communications point of view and a collective point of view, if we feel powerless, it makes us more passive, if not more depressed. Empowerment is very much part of effective implementation, and empowering includes acknowledging differences. And again, I'm not a health specialist, I'm a communications specialist, but these are all things that need to be asked.

Vicki Lemieux [00:13:36] Yeah, I think so many good points.
Vicki Lemieux [00:13:39] I think, you know, what your last point reminded me of is the political theory of voice and exit as well. So you said, you know, if we feel powerless, we are more passive and have a tendency to be more depressed.

Vicki Lemieux [00:13:55] And also people, if they haven't got a voice often will exit in various forms from social contracts, for example. And so you have a less engaged society and you have a society where which I think becomes more polarized as well. You've got a couple more minutes. And I wondered if you wanted to just address a couple more of the questions that are coming up in the chat. There's one about universal basic income as a proposition for everyone to act as a catalyst towards more equitable social justice. And then another one about health research there. There's an important role for patient partnerships in research. So if you have comments on any of those at all.

Nora Weber [00:14:53] Well, Michael's question about patient partnership, must take into consideration the role of dominant colonialist thinking. I know, by the way Michael has posed his questions and comments, that he's conscious of these things - but we're so unaware of what we're unaware of. And that's where it's important that the patient partnership ensures we leave space for people to bring in their perspectives (in a way that is meaningful to them).

I'm working with Chandana on communicating about an opioid app. We're aware that it includes the Downtown Eastside and communities like that, and the disadvantages and the health complexity of those communities. There's unconscious bias and some people have spoken about that, but there's a real tendency, if we're dominant, as either researchers or colonialists or however you want to put it, of not really hearing nuanced concerns. In communications theory there is this whole thing of direct communication versus nuanced communication (in low context versus high context cultures). In some cultures, it's the unsaid that you listen for, not the said. And we don't come from one of those cultures. So how do we partner with cultures that do come from that, like Middle Eastern cultures or Indigenous cultures?

Vicki Lemieux [00:16:43] Yes. Very good, very good point. So we'll leave it at that to reflect on and perhaps leave a lot unsaid and I'll turn it over to Kohei now to carry on.

---


49 Suggested reading

Vicki Lemieux [00:17:00] And I'd just like to say he is coming to us from Japan.

Vicki Lemieux [00:17:08] This has been, I'm sure, an exercise in absolute endurance for you because you've been up through the night listening to this conversation. So my deepest gratitude and respect to you for staying the course. So over to you, Kohei.

Kohei Kurihara

Kohei Kurihara [00:17:25] Yeah, I'm very glad to be invited. This is great opportunity to join with you and all these speakers. Also the attendees we see from very amazing backgrounds. My name is Kohei, I'm from Japan.

Kohei Kurihara [00:17:39] It's early time, but I'm very excited to do this again just to having conversations. My background, I've been working on the blockchain space. One of the American non-profit, the Japanese chapter leadership here. Also, I'm working at startup, which is developed with self-sovereign identity capacities. As I'm based in Asia, and this market, so I want to talk and started about the data protection in Asian perspective into the crisis situation and coronavirus. A lot of Asian country is in a very strong stance. The Government, it has tried to collect the data such as in China, just South Korea and Taiwan is gathering citizen's data to centralize ownership. But they are very successful things so far. Like in South Korea, it's been like infections in this moment because the government is tracing it on tracking records of the citizens. But again, in Japan and Singapore is a bit more privacy protection style. But they're missing the opportunity. In particular here in Japan, in Tokyo. It's been a gradually increase in numbers of infections. The Asian privacy protection style is different, even in our own continent. So that such as an interesting in Japan, we are facing many things right now at this moment. We try to update our own data protection law. Maybe it will be started in the two years, right. Is now always in discussions. But the problem is here, all our data protection legislation is very flexible compared to the GDPR. It's not just a compulsory or the private companies also think the government has no reasons to disclose the all information and data to the Public Citizen's. Therefore, we need to make more fighting against the practical appearance, in particular in the private sectors.

So that's the time that started to work with this. More the camera. These are the privacy protections we gather the main industry. People do also. There's some other initiatives that the people want to be concerns, too, to monitors the government actions after the data coronavirus. They also do I'm talking with the some other Asian countries such as India, South Korea. They did the like the privacy virus, a lot of the things before the
government. But they have their own the law. I said it looks like the South Korean GDPR, all they try to figure out what the best practice for the government actions against the civil initiative. So this kind of activity is enough coming, this moment in Asians. The data protection landscape. I think it is the kind of the concept that is very interesting. I think it's very different from the Western topics, but we have many opportunities to work together and also to make more strengthen the system to fight against the public sectors, to use our own data without any consent.

Vicki Lemieux [00:21:34] Thank you, Kohei. So it is really interesting to have that perspective from Japan. And I know you've been working on different blockchain technology. I didn't get a chance to type in the chat, but I would like to. It's come up and this is in reference to some of the earlier conversations about self-sovereign identity. So you're familiar with that technology. And there are different varieties of self-sovereign identity technologies, different varieties of blockchain technology.

Vicki Lemieux [00:22:10] So I'm wondering for you what is the type of self-sovereign identity technology that is truly privacy preserving and the kind of approach that would work better in this instance versus maybe some other approaches to the technology that are less useful in this context? Do you have any reflections on the different varieties of blockchain and self-sovereign identity technologies?

Kohei Kurihara [00:22:45] I think the self-sovereign identity technology has the great potential, being compared to the centralized database. We have seen in many tech such as a Sovrin, has been for an active space and Hyperledger is the very promising space. Also, there's some other economy has been developing and these technologies finally. So I think the self-sovereign is that a very important to try to figure out the privacy protections in additions we need to consider how we can make an app disseminated to the market. Because the we work in and we stay private company in Japan, but they don't know what is self-sovereign means we need to many times to convince them to work with us together. Of course, the technologies are very important regarding the privacy perspective, but that the problems is that a lot of the companies don't know how to use this technology for the privacy protection. So that's why do we need to some lead times to convince them this technology is a perfect deal. So we need to give them a benefit with regional experiences for their users. So it's that that's why we're talking now. We see private companies... they have their own economic barriers. They can make privacy protection as well as the day to day on the business part. So we really see why work on this space, not just only for the critical perspective, but also the business benefit or the companies.
Vicki Lemieux [00:24:33] Yeah, that's a very, very good point. That hasn't been raised thus far.

Vicki Lemieux [00:24:39] I want to bring you back to this notion of the usability, because one of the issues that has come up in my own research is the complexity of self-sovereign identity technology for the end user. Things like private key management, leading to know how to properly be the custodian of your own private key and protect it. And so, the challenges of understanding cryptography and how it's used in these types of solutions. So, I'm wondering if you've come across those challenges and have you seen examples of how we might overcome those challenges?

Kohei Kurihara [00:25:34] Yeah, that's a good point too what we are try to solve this issue. But we haven't seen any specific directions. But the futures, I guess, did the private key. It's been a strategy to sell. Right. Just to kind of biometrics to what any other detective processes could be worse. You don't have to be care about the like holding a private key. It's you know. So, what was it happens. It's been a more protective.

Kohei Kurihara [00:26:05] And so did this is the most promising technology will be coming out.

Kohei Kurihara [00:26:14] So you naturally go anywhere through our bodies to work through your gestures at something. So, they just kind of this seems to be the future alternative to hold to the private ticket in private keys instead.

Vicki Lemieux [00:26:28] So is Michael Cholod right in saying that maybe it's an architecture question, you know, how do we know that some of these challenges that we see now are really just about considering how the technologies need to be architected in a way to preserve privacy and address some of these challenges. Are they all solvable through technology? Or do you see any limitations there?

Kohei Kurihara [00:27:01] Yeah, I think the architectural solution is one of the data protection approach.

Kohei Kurihara [00:27:10] But the problem is that we don't have to compromise to use these, abilities because we did take for example in Singapore they are try to make a fully compound privacy architecture of coronavirus apps. But the problem is their application has not been in like to spread out to the citizen just almost along quarters. It's not been enough, the numbers. So, we always discussed it. Whether this technology could be used to among the people we've been discussing just more than almost to two
years. Of course, the technology is a very important privacy protection, but we need to know biases of these abilities. So, I think at this point, it's a very important deal. Also, we have to put on the tables. What is a benefit for the users with the privacy protections, right?

Vicki Lemieux [00:28:12] Yes. I feel like sometimes individuals, you know, they'll trade off privacy to have usability and, you know, regret that decision later. Or maybe because it wasn't a decision. It was on the spur of the moment. What about, you know, this idea of interoperability that has come up and the need. Are we looking at individual kinds of ecosystems that are kind of walled gardens? Or do you see more of an ecosystem where it's like the Internet, where there's interoperability and it's more open and fluid?

Vicki Lemieux [00:29:04] How do you see that evolving that space?

Kohei Kurihara [00:29:04] Using the data for the interoperability, we have to talk together with a lot of other backgrounds because the supplier to many people isn't in a different petition's. The means it was not happen any convincement. So that's why do we need to start to consider it as standard is a different background. This is not just a technical problem it is just like kind of the social inclusions. So I think this is a very important to make making the pressmen clear at the lot of the people can easy to join together.

Vicki Lemieux [00:29:52] Well, yeah, really good point. Really good point. Well, let's end on that point and thank you very much for your reflections

Kohei Kurihara [00:29:52] Thank you.
Vicki Lemieux [00:29:52] I'd like to now pass the baton again, this time to Ma'n. And Ma'n are you there?

Ma’n H. Zawati

Ma’n H. Zawati [00:30:18] Well, first and foremost, thank you very much for this kind invitation. I mean, it's really tough. It's a tough job to be one of the last speakers, especially with everything that has been said before. But I want to really, truly thank you for organizing this and keeping it on time. Thanks to Michelle as well, for all her for all of her help coordinating.

Ma’n H. Zawati [00:30:46] As I said, being one of the last speakers means there's a lot that's been mentioned already.
Ma'n H. Zawati [00:30:55] But maybe I'll start with a bit of background. I'm the Executive Director and Assistant Professor in the Centre of Genomics and Policy at McGill University. My background is in law as with many colleagues on the call. Over the past few years, I've been interested in mobile health apps. Of course, we've talked a lot today about mobile health apps, especially contract tracing apps. But I think there is a kind of application that deserves more scrutiny these days, and those are symptom checker apps.

Ma'n H. Zawati [00:31:29]. It's really important for us to keep in mind that the issues we're all seeing preexist the present moment. The current pandemic has exacerbated certain issues, but also helped us to identify lagging concerns that we've been grappling with for quite some time. If you look at Canada, for example, recent numbers suggest that 81 percent of us use mobile phones. If we look at the mobile health applications sector, it's grown 87 percent faster than the mobile industry as a whole. In total, close to 450,000 mobile apps currently exist.

Ma'n H. Zawati [00:32:21] Of course, mobile health apps are being widely used.

Ma'n H. Zawati [00:32:27] By 2024, we're expecting almost 3 billion downloads per year. We're also expecting the digital health market to exceed five hundred billion dollars in revenue. Now, we'll see with the pandemic how this is going to affect that number. But it's clear that the issue is massive. It's also clear that when it comes to mobile health apps, we can't think of them in a one size fits all approach.

Ma'n H. Zawati [00:32:51] There are, of course, health apps for tracking and health apps for general information. But as I mentioned, I think that we need to be paying much more attention to symptom checker apps.

Ma'n H. Zawati [00:33:02] These are applications that have existed for quite some time. They make up close to 7 percent of health apps currently on the market and are available on app stores worldwide. When compared to tracing apps, many of which have been specifically developed for COVID-19, many symptom checker apps, such as WebMD or ADA have simply decided to expand their functions to include COVID-19. The pandemic raises a number of questions, especially because symptom checker apps can essentially be built from scratch and don't often get subjected to public consultation and so on. The pandemic, in other words, did not really allow us the time to develop new apps and new app functions properly.
Another issue is that for apps that have added pandemic-related functions, there were preexisting terms and conditions that weren’t developed with the current health emergency in mind. Adding to these problems is that mobile health is quite unregulated in Canada. Health Canada released a regulatory statement on software as medical devices, but many symptom checker apps would not fit the definition of a medical device, depending on exactly how they function and the kinds of data and images they capture. Aside from Health Canada’s guidance, there isn’t much regulating health apps. And this is a problem because we’re seeing a lot of issues with them. For one thing, their accuracy has not been clearly established. These apps also have unclear policies and practices surrounding data sharing.

A 2019 study\(^{50}\) for example, looking at apps from Canada, the US, and UK, showed that apps are often marketed as empowering patients and users, but they tend not to give them much control at all over the ways their data is used. Users can't choose the precise kinds of data that the app can access and use. And then neither do they give an option for users to opt out of particular uses. Another complication is that many symptom checker apps are not actually used. These applications apps are not targeted only to consumers, but physicians sometimes also recommend them to their patients. And a lot of issues related to privacy, specifically around data sharing, have not been a question of discussion within professional, medical associations. One of the big problems is that people do not look at the terms and conditions, which most of the time are very long, and they’re often not very easy to find. A user would have scroll through a large body of text that’s likely written in inaccessible language.

Ma’n H. Zawati [00:36:50] Even when they exist, many app privacy policies aren’t very clear. We don’t have much data about how many people read and understand entire privacy policies. But we do think that when people download a new application, they have a tendency to treat it like a game. “I really, really want to just get started.” So they signal that they agree with the policy. But again, we don’t have much in the way of empirical data on this. Recently, an app promoted by Alberta’s government for managing COVID-19 care faced some controversy and is now under investigation by the provincial privacy commissioner. It’s called the Babylon app.\(^{51}\) This app stated in its terms of conditions that the developers are entitled to share user data with members of


the corporate group and with their partners. It also states that personal data may be made accessible to foreign governments and agencies.

Ma'n H. Zawati [00:37:45] In fact, when we've looked into who is behind many of these new COVID-19 apps, some foreign governments came up. So these are the kind of apps that have been rolling out during the pandemic. There’s, of course, a lot of haste, but there could also be COVID-19 opportunities. Perhaps when we think about the capacity of governments to legislate and protect us, we may need to change our frames of reference.

Ma'n H. Zawati [00:38:27] For one thing, agencies like the FDA or Health Canada are not going to be able to regulate all of these different applications. It’s just not possible. Understandably, these agencies are probably going apps that pose higher risks, which perhaps opens the door for other government entities, such as consumer protection bodies, to step in. Consumer protection bodies may be able to address the misleading information provided by these apps. But we should also think carefully about the role of professional associations. A lot of these applications play a significant role in people’s health decisions.

And specifically during this time where we're not really able to visit a physical clinic, we might see an increased use of symptom checker applications. So, we need professional associations, medical colleges to step up and be involved in this discussion, to give guidance to both professionals and members of the public. And when a clinician recommends or prescribes a symptom checker application to someone, for example, they need to be able to explain the privacy risks and other issues that might come up.

Ma'n H. Zawati [00:39:53] Another thing I think we need to keep in mind is education. We’ve been discussing this a lot today: civic engagement is a must.

Ma'n H. Zawati [00:40:09] And this in this era, and not only just engaged in by providing information, but also providing tools to help people make decisions on “well, that one doesn't really seem to fit, the bill.”

Ma'n H. Zawati [00:40:23] “A lot of the things that we have to be looking for, I can’t find them on the application. Therefore, I'm not going to be able to use it.” I come from a world where ELSI (the ethical, legal and social issues) is the terminology we use.

Ma'n H. Zawati [00:40:38] I think we need to add a P for psychology as well. We need to be able to learn a little bit about people's decision making process when it comes to looking for information about their health and how this impacts decisions about using
symptom checker applications and the threshold of risk when it comes to their privacy. I’m happy to take your questions.

Vicki Lemieux [00:41:08] Thanks so much, Ma’n that that is really, really some very interesting ideas in there.

Vicki Lemieux [00:41:14] I think you’ve got a question from Michael in that in the chat and then some questions from me as well if you care to address them.

Ma’n H. Zawati [00:41:21] Sure. Do we need a Canadian Consumer Reports for these apps? I think that we do need some form of reporting. But the question is, how do we do this efficiently? There have been several initiatives for creating some form of registry of applications. And nothing as of yet has been successful because of the sheer number of them. Another option that’s been tried, but which hasn’t necessarily been successful, is to have an entity, a body within the health sector, that monitors these applications.

The UK’s NHS, for example, built a registry of vetted applications. In this case, the vetting process conveys some form of credibility for these applications. But the initial steps toward that has been very difficult. And there are a lot of applications that were deemed not credible even if there were included on the list. I do think that some form of registry would be important, but perhaps the best way to allow this would be to ensure that the consumers and users have the tools to assess and make informed decisions. And so one way to go about it, because of the number of applications out there, would be to provide a checklist of things that users should be looking out for. If five out of 10 elements are not included on an app, it would really reduce its score, meaning that users might avoid using it.

Vicki Lemieux [00:43:21] Yeah. I wanted to add to that same line of discussion you mentioned about the associations taking a stronger role. I’m wondering if, like in the financial sector where there are self-regulating bodies, if this is also needed in the health care sector, to develop similar mechanisms rather than it’s a being always government to step up.

Ma’n H. Zawati [00:43:53] I absolutely think it can’t just be governments. Soft law, for example, has much more flexibility in terms of what we can do and how quickly we can do it. So I would say the best approach is to have a mix of both.

Ma’n H. Zawati [00:44:12] You need some kind of a binding approach, but you also need a kind of a community-based approach. In this case, professional associations could play a very important role in achieving that. I think these are all matters that we
have to keep in mind. I saw one comment about the Alberta reading index. I'd be more than happy to be able to take a look at that and provide feedback. It's a really interesting approach.

Vicki Lemieux [00:44:43] And just I just wanted to dig deeper into the issue of self-regulation.

Vicki Lemieux [00:44:48] I know from the work that I've done previously in the financial sector that one of the problems in the 2007-2009 financial crisis is that the self-regulating bodies had basically been, I guess you could say, sort of occupied by certain large economic interests like the banks. And so, you know, there's something to be looked at in terms of how do we make sure that those bodies, if they are self-regulating, are then, you know, operating in a manner that is not necessarily taken over by lobbyists or powerful interest groups. And have you thought about the structure of how this would work at all.

Ma'n H. Zawati [00:45:40] Yes, I think this is a very important point. And I think this needs to be done in some form of collaboration between the different groups, which could be self-regulating, but with other with other stakeholders included as well, such as in academia. I think one of the issues that we're facing, which is unfortunate, is that there is a power difference when it comes to the use of these technologies, especially mobile apps. There have been quick advances from the technological side and the prospective action done by legislators and other regulators has been slow, which has made it really difficult to address the matter in a well-framed legislative approach, while also being adequately nuanced.

Ma'n H. Zawati [00:46:39] I'll give you an example of the power dynamics at play here. Many mobile health applications not only do tracking and symptom checking, they also do research. If we look at Canada, for example, the requirements for research, especially in provinces, is that you need a REB to make a decision on recruitment.

Ma'n H. Zawati [00:47:17] But there is nothing that, in the past, stopped developers from using these apps to recruit individuals without a restrictive export. There really was no oversight. And some of these large companies, for example, after consultation with researchers and academia, actually made changes to their developer agreement and required that developers building an app for research to first obtain ethics approval. And so this has really shifted the power relationship. It was really in the hands of the companies because there was nothing powerful enough to provide adequate oversight. And some of the rationale for this came out of conversations and consultations within
the company. Other sectors of society may think this is probably the model that we
would like to go for: an involvement and an engagement that is interdisciplinary.

Vicki Lemieux [00:48:38] That's a good point to make a transition. And to our next lead
witness who is coming from yet another discipline.

Vicki Lemieux [00:48:47] So, Noelannah Thank you, Ma' n, for your interventions.

Vicki Lemieux [00:48:50] And Noelannah, I'm going to turn it over to you now to speak
about your perspective on this topic.

Noelannah Neubauer

Noelannah Neubauer [00:48:57] Thank you very much, Vicki and thank you you all for
sticking around for an incredible day of conversation. And I find that this has been quite
enlightening. To give you all a little bit of a background on myself. I am a postdoctoral
fellow at the University of Waterloo out of the Faculty of Applied Health Sciences. My
background is more so within occupational therapy and kinesiology. My presentation will
serve as a follow up from Dr. Liu's presentation this morning on this concept of
dementia related wandering and its use of self-sovereign identity.

As noted by Dr. Liu, missing persons involving persons with dementia is continually on
the rise. And the use of monitoring technologies has definitely been of considerable
interest when trying to keep this population as safe as possible. And we're starting to
see more and more in monitoring technologies above and beyond just this just this
particular population. With the use of monitoring technologies, however, as has been
discussed, come with the risks of privacy and security of the person being monitored.
And our group truly feels that self-sovereign identity could be a potential solution to
mitigate some of these risks. But before we can begin to even evaluate the usability as
well as how SSI could be implemented within the health care context, we must first
focus on how we communicate this concept to the public. Other than the small
percentage of individuals that do work in this area, very few are actually able to
conceptualize what exactly self-sovereign identity is. I for one, not that long ago didn't
know what SSI was. It took quite a bit of information and learning on my part due to my
health background.
As part of my Mitacs funded project\(^{52}\) that I'm doing here in Canada that I've been working alongside a start-up company called Secours,\(^{53}\) I've been working quite closely with persons that live with dementia and their care partners to come up with some form of a term or a better way of being able to identify what exactly self-sovereign identity is so can be better understood by the public. So basically what I've done over the last couple of months is I've looked at using a hybrid model for concept development which entailed ways me looking deeply into the literature, seeing how people are using SSI, then breaking it down into a couple more digestible components as to what makes SSI, SSI. In this case of course, ownership and control, decentralized authority that we've been discussing today, privacy, digital identity and security really are the key components of what makes self-sovereign identity.

What I did was I take those five different components and then used them when I did a series of semi-structured interviews with persons that lived with dementia and their care partners. During these interviews, I asked them what they thought of the concept of SSI, and if they knew what it was. After I explained it to them, participants thought of SSI as something that is of interest to them and they were really excited as to what SSI could potentially offer to protect their privacy. The fears that are derived from their data being hacked of them being preyed upon is something that is very real for the older adult population and the participants that I interviewed. One of the persons with dementia, for example, that I spoke to, he unplugs his modem every single night from his computer and he avoids the use of social media just because he's mortified that someone's going to take advantage of him. He said that the use of SSI could definitely increase the opportunities and be more invested in monitoring technologies if he knew that his data and his identity were protected. It was unanimous, however, that no one, when I interview them, had any idea as to what SSI was before I explained it. In fact, when I was trying to recruit participants, it was quite difficult just because this concept is something that's very new. There's almost that fear, that unawareness as to what it could potentially offer.

And when I use these individuals in the interviews and then brought them into a series of focus groups and asked them to come up with something that would make more sense, they came up with three basic words that could be tied with SSI. Those three words are secure data ownership. So if they go ahead and speak to their friend or I spoke to my grandmother and said that self-sovereign identity is about secure data ownership it would help them get a better understanding as to what exactly we're talking


about. To be able to tie this into today's witness seminar with COVID-19, we all know that there will be a greater push in the tech sector for monitoring technologies.

However, we really need to keep in mind that there remains a fear among members of the public, including our older adult population, that these technologies will increase their risk of being preyed upon. While coming up with the solutions to mitigate these risks such as SSI will definitely be essential. And again, this was iterated over the last couple presenter's, which is exciting, we really need to keep in mind the importance of education and awareness and ensure such solutions can be successfully adopted. Adoption is critical. We can develop amazing technologies, but if they're afraid of it and they're not willing to use it, then what's the point of developing the technology? As highlighted this morning by the honorable Joyce Murray, when dealing with privacy concerns, we must first have the trust of our citizens. To do this, I propose the following. The first one is to echo from Paola, Nora, and Michael's point this afternoon, we really need a greater emphasis on participatory approaches. The network that Dr. Liu and I are a part of is called AGE-WELL NCE. AGE-WELL really focuses on the aging and technology sector and they provide perfect examples as to how you're able to bring older adults and other members of the sector in and provide meaningful engagement on the development of the conceptualization of the technology. But really, as we're moving forward. How do we find ways of including them at the conceptualization of the technology through to the deployment phase? And then even after the technology has been deployed, how do we ensure that their voices are continually heard and that their concerns are able to be further implemented within these technologies? To further echo from what was noted by Nora is that there is definitely a need for interdisciplinary teams.

We've been speaking a lot about public policy but bringing in allied health care professionals such as occupational therapists could be another key component that we need to look at. OTs are experts in usability testing and for providing advocacy among their clients. This is something that we should really look at moving forward. But of course, how do we reduce these existing silos? This is something that we always end up talking about. And then as well, if we're trying to bring individuals from multiple different sectors together, we all have our own different languages based on each profession. As a health research, I struggle to understand the terminologies that are used by computing scientists and engineers and it works the other way around for them understanding the various health terminologies I might use. So how can you come up with a more universal language when we're talking about privacy?

Vicki Lemieux [00:56:43] Fantastic. Thanks. Noelannah and great research that you're doing and also great ideas for how we can move things forward. So I just wondered if

you had. Well, first of all, there was an earlier comment from Nadia about wearables that, you know, the research area that you're looking at.

Vicki Lemieux [00:57:07] I wonder if that has come up in your conversation that is asking, you know, do we if we reach a threshold that blurs the difference between consumer device and medical or therapeutic device, and that certainly seems to be something that we need to look at in the context of COVID-19, but in the analogous context of Alzheimer's in older adults. And then I just had a question around, you know, who else do we need to include in a conversation to carry this particular conversation forward? In your view?

Noelannah Neubauer [00:57:39] So I was actually hoping I could answer Nadia's. I was quite excited when I read it. We've already hit that point where pretty much there's it's dissolve between health care products and then those within the market, persons with dementia that I speak to keep them safe. There are some that have received health Canada approval. But again, because there's so many different hurdles that companies have to go through. We are very quickly moving to where things are being available off the shelf. But then what Lili had alluded to earlier about this aspect of data and how we have no idea what the prevalence is of missing persons with dementia. The problem is, is that we really want to get some of these technologies like GPS devices subsidized. But we can't do that because they're not deemed as a health care solution.

And we want to be able to go forward to the governments and show them it could be effective. But again, there's that massive issue with data. SSI could be a salutation to that. Another key component that we would love to see is seeing some of this information that's being collected, being sent to researchers such as Dr. Liu and myself and being able to use some of that data to be able to help to subsidize some of these different technologies that have reached mainstream rather than having to try to find companies that have applied for health Canada approval for their devices.

Noelannah Neubauer [00:58:58] Hopefully that answers it.

Noelannah Neubauer [00:59:00] And then in terms of Vicki, your question on other people, we want to expand on moving forward. So I always end up liking to use things like ecological model, all the different sectors that are touched by it. So our work that we've done over the last couple years, while we involve persons with dementia, we always want to involve anyone else that is touched by that piece of technology. If I'm involved with someone with dementia, the next person that has that kind of sphere of influence is their care partner. But then above and beyond that might be their families. And then we extend that.
We're talking about the Alzheimer Societies and the community organizations being a level up from that. Now we're talking about police in our case and then even higher, we're talking about policy. So really what we feel is that you need to involve all those different levels, because if there's one hiccup in one the levels, it's not going to transcend to the top. And we want everyone truly to be involved in that.

Vicki Lemieux [00:59:51] That's a very good model. Very good point. I think it resonates with the point that Nora brought up earlier about eco districts, if you will, from a different disciplinary perspective.

Vicki Lemieux [01:00:07] So Nadia I think just responded to your last comments and perhaps you want to just to respond again to.

Vicki Lemieux [01:00:45] Nadia, go ahead and open up your mike. It's just faster.

Nadia Diakun [01:00:50] Absolutely. In the 1990s, our mechanisms were we weren't that much of technology that we could rely on. So you didn't have technological solution, but there was certainly a legislative instrument solution. And those three pieces of legislation were to balance out what the province had been trying to do for the 20 years prior to that. So this was the NDP government and the Advocacy Act was that they were interlinked. So, for example, if I, as a caregiver of my elderly parents, I could act as their advocate. I could hold their powers of attorney for consent to treatment. I could hold a power of attorney for substitute decisions in, you know, for a property, etc. If you were to look at those the intention of those three pieces of legislation, look at what we have today. Currently within the province or any province and see how SSI might actually be the technological bridge that would make it possible to affect all of these roles that a caregiver may have or perhaps, you know, a loved one could have just a thought.

Noelannah Neubauer [01:02:07] That's a really good thought. I know Dr. Liu is listening on the other end and she's probably taking notes as well that we need to look at that. So thank you.

Vicki Lemieux [01:02:15] All right. Well, thanks so much. Noelannah and Lili in the background there. And so really appreciate your your interventions. And I'm going to now turn to Ajit. Ajit. Are you on the line?
Ajit Babu

Ajit Babu [01:03:00] Well, thank you. Thanks so much, Vicki. And let me say that it's been an outstanding experience from my standpoint. Really scintillating stuff and quite distinct from the things that I normally get to hear about. I really wish to express my appreciation for all the participants and the diverse points of view that they brought to this very important topic. Being the last one of 20 odd presenters. I think you will forgive me for not perhaps having any great insights into this problem, but I did want to share my thoughts and sometimes that can be helpful, particularly since I may have a perspective that, you know, may not have been brought up so far. When I look at problems, I try to break them into triads. I like the fact that there may be three of something. While reflecting on this topic of “Can governments respond to COVID-19 and still respect personal privacy?”, the words that came to me were three, of course, with the first being perspective, which I just mentioned already. The second was value. And the third was expectations. So - what does this mean? If you look at perspective, naturally, we all look at things from certain perspectives - and not just one, but a number of perspectives depending on which hat we are wearing at the time. The perspectives that I'm in the best position to allude to are, naturally, the ones that I myself have. So, from that standpoint, let me share with you a little bit about my background. I am based in the United States in St. Louis, Missouri. I'm a professor of medicine. I practice primary care. I see patients on almost a daily basis, largely in the outpatient setting, sometimes inpatients as well. I've been a funded researcher, both in the United States as well as in India, where I do a fair amount of public health work, which is really based on planning. I've also been on an institutional review board, so I've sat in reviewing research work, especially from a standpoint of privacy, confidentiality and ethics.

Looking at all these perspectives, in a given moment, the way that I might decide to view something might vary, very substantially. When we've talked so much today about the COVID-19 pandemic and the different ways in which we might need to approach issues like privacy and taking care of this epidemic, one of the things that I don't think we discussed very much was just the real impact on people. The people who are out there. I see those kinds of people practically every day - though now I don't “see” them as much because I'm doing tele health! After 30 years as a physician, I get to actually sit at home and work on the phone with the patient and try to take care of their needs.

When you work directly with patients, you see that the things that concern them may often be very different from the things that concern, you know, a larger entity like the government or researchers or perhaps even society at large. Each individual has their own concerns. And depending on the perspective of “I'm a primary care physician and I'm about to go see a patient” … I'm gowned up in a yellow gown and I've got my eye
protection on and I've got a mask on and gloves on because the patient came in with cough and shortness of breath and I don't know if that patient has COVID....I'm about to turn the doorknob and go into the room and I hear them coughing on the other side and I keep turning the knob and I go in.... That's one perspective. That's what I see as a doctor. And that's what the patient on the other side of that door who may be afraid of what ultimately I might have to tell them is facing.

On the other hand, then we move on to the second word, which would be value. And how we view it depends then on the value system that we have. So what value does our society place say on a human life versus a job? What value does an individual place on their own life or the life of a family member versus their need to have a job and put food on the table? And what value then does such individuals or societies place on things like privacy or knowledge or education or equity? Sometimes those discussions and concepts are driven by those who are towards the top of the pyramid, not necessarily the ones at the bottom. In general, I believe that values tend to be sort of ingrained in a nation or a society. They may not change very dramatically even though we are facing an unexpected challenge. This brings me to expectations.

So the expectations that we might have, I think, do change sometimes very drastically based on the kind of situation and the context in which you're facing it. A number of the prior witnesses alluded to context. I certainly believe that context is extremely important in looking at any problem. So I'll give you a couple of tangible examples from my patient care practice. We run a walk-in clinic, which sometimes I supervise. We typically see about 20 patients a day and we were seeing patients who were coming in on a regular basis for that. Some of them have very mundane complaints. Some of them have really genuine complaints. Some of the complaints made us wonder why they didn't come in earlier. But now, instead of seeing about 20, we are seeing two or three a day. And we have not put a specific curb on visits. It's just that people aren't coming in. That's point number one.

Point number two, I stated earlier that I have phone visits with patients, addressing issues and complaints, and taking care of them over the phone instead of seeing them in person and touching and feeling and ordering tests and doing the things that we normally do for the most part. In fact, almost invariably patients are quite accepting of this. And more than once patients are asking that they would prefer not to come in so can I do something over the phone? Why are they doing that? It's that's because their expectations have changed as to what they would like me to do for them. And if I had to choose one reason for that, the dominant reason, I think, is fear, because they are afraid. They're afraid of contracting the disease and they're afraid of being put in a position where they may be the next person who gets it. That fear is prevalent not only
among individuals, but even among societies and governments and around the globe. It has triggered a lot of the actions that we have taken which have acted as a catalyst for many things that we had done, some of which are extraordinarily good and some maybe not so.

But ultimately, I think the context of these three words, perspective, value and expectations really would need to inform the discussion of where we go and how we go. For example, since a lot of my work is in India, I have seen that they have done a great deal in trying to limit the potential of COVID. There have been fears expressed around the world of what it would be like if such a populous nation as India with the weaknesses of infrastructure and other resources, may have a rash of COVID all over the country. But they have done tremendous work to try to reduce this in their own way. So, for instance, the prime minister speaks and with three hours’ notice shuts down the entire country. I don't think that would have flown very well in the United States. I don't know if the United States could have even managed something like that. But India somehow does.

And that is one of the strengths of that country, that despite weaknesses it may have in infrastructure and resources, it manages to keep going through adversity and come out ahead. We talked quite a bit about contact tracing and possible privacy issues relating to that. And, of course, concerns of inappropriate use of information, perhaps the stigma that might be associated with being tagged as somebody who has contracted it. Again, in India, for example, in the place I am connected to - which is the state of Kerala - they have extensive measures in place to try to trace people. They have had a total of four fatalities so far and just a few hundred cases, despite the fact that they have tremendous numbers of people coming in from places like the Middle East where there's a huge expat population and where the disease has been quite active. They have publicly notified even individual houses as being the residence of somebody who has gotten COVID-19. They put signs in the street specifically identify the hotspot. Imagine, therefore, what privacy is that homeowner having when everybody around knows that there is an infected person residing there. But on the other hand, the people around that home are happy in the sense, OK, at least we know where the infected person is and we can take some precautions of social distancing and saying away. In many cases, the homeowner themselves are accepting of this as being something that is part of the societal intervention to deal with a problem like COVID-19. It's just a revealing, you know, having had that opportunity of living and doing things in two societies in pretty close proximity in time.

Ajit Babu [01:12:48] I was there in January as well as February and could see the tension of how things like perspective, value and expectations can really color the way
we approach a problem. So, to summarize then and come back to the fundamental question for today's discussion, can governments respond to the COVID-19 pandemic and still respect personal privacy? I think the answer is definitely yes, they can respect it. Now, what does the word “respect” actually translate to and what does “privacy” mean? Because even some of our participants referred to the fact that privacy is not one word that fits all. There are differing definitions and perspectives that may inform us as to what is privacy and to me it ultimately boils down to context. I have chosen three words, perspective, value and expectations as to what would influence the optimal way forward. But I do feel that now, at the end of this seminar - compared to the beginning - I feel definitely more optimistic that people will not necessarily have to have a trade off all the way. Sometimes you would think, well, I'm giving up privacy and so I'm getting more efficacy or I am giving up efficacy and building privacy. But I think with the things that I've learned more about today, like self-sovereign identity and blockchain and some of the technological approaches that people like Nadia talked about, it really makes me feel that our technology can help us to get to a point where we're getting what the average person and a reasonable person would think is very good efficacy without having to make significant compromises in privacy. So with that, I think I will conclude my remarks, but I'm happy to look at the questions and to add anything to the discussion.

Vicki Lemieux [01:14:49] Thank you so much. It's very difficult to be the last speaker in such a marathon. Zoom-a-thon, as Michael earlier called it. And I think, you know, your comments both really brought it back to a kind of a real place as a clinician who is dealing with patients who might have COVID-19, who are experiencing fear. But also, you know, beautifully summarized the fact that through some of the interventions we've had today around tech new technologies, that there is hope. And so it doesn't have to be this this kind of binary tradeoff. So a lovely last intervention that left us on a hopeful note test, which I very much appreciated.

Ajit Babu [01:15:39] Thank you. I see that you put in a question here whether there is a different baseline expectation around personal privacy in India versus the US? In usual times? That's certainly a very relevant question.

Ajit Babu [01:15:53] And I would say the answer is definitely yes. In that, of course, the United States has great expectations of individuality. So individuals in this country really expect that they will have privacy and freedoms and be able to do things they desire to a very significant extent. While in India, the typical person does not have any such expectation. The people who do have that expectation and perhaps to inordinate degrees, are the ones who may be influential and affluent. They seem to believe that society can essentially be twisted to their image in any way they want. And sometimes
they are successful in doing that, but they are definitely used to that difference in perception. Some of the kind of discussions we may have about privacy or the fact that we're giving our information without explicit permission is something they're not even bothered about because they are either not aware of it or because their sense of value and their perspective is different.

They're looking for something that makes life easy, that might give them a return of time or money or investment. And in return for getting that, somebody somewhere is tracking some data. In a way, they didn't get a freebie. They got something because they were giving back their information, perhaps not with any obvious consent. But that is what the transaction was. There was a transaction there, which they may not have been aware of. They gave something back in terms of their privacy and their data, which is being monetized or being used for some other purpose by whoever got it. And that's just the way it is. So, some of the discussions we had today and some of the concerns raised would be regarded with great perplexity by them. But that, again, is very context based. I would also say, in conclusion, that even though there's a Canadian perspective, no doubt, in this discussion being hosted in Canada, we can see how this pandemic is a very important example of how the value system and the culture and the beliefs of a society at the other end of the world have led to circumstances that have come right to our doorstep today and are affecting literally our daily lives and and our safety.

Vicki Lemieux [01:18:27] Yes, absolutely. And I think, you know, it's really important to bear in mind it's come up several times. The issue of context and that is you said very aptly that, you know, some of what we've raised today and some of the concerns raised would be quite perplexing in different contexts and that there are a diversity of perspectives which, you know, I'll move now and to wrap up our conversation as we've reached the time for me to just to just sum up.

Victoria Lemieux, Vote of Thanks to participants
Vicki Lemieux [01:19:01] And the only way that I could possibly sum up such a diversity of perspectives is to just thank you for bringing such diversity of perspectives to this issue. I do believe that greater understanding, innovation, the solution to problems does come from looking at issues from multiple disciplines through multiple perspectives. We've talked about inclusion, making sure that different voices are heard, and that reflects what the Peter Wall Institute for Advanced Studies at UBC really stands for, as well as bringing together these multi-disciplinary conversations so that we may learn from each other. I've learned an enormous amount from each of you, and I am deeply grateful. I'm amazed and surprised that everyone pretty much has stayed the course. So thank you again for being such great, great witnesses in this witness seminar, such great participants in this process. It hasn't been without hiccups. I think it's been a bit of
an experiment in how to respect people's privacy, but still engage them in conversation. So in terms of process, I think I've learned something there as well.

Vicki Lemieux [01:20:24] But I would just like to again, just thank you for your generosity to all the lead witnesses for your time. I know everyone is very, very busy. And for the participants, for your patience in the process and your contributions in terms of questions as well.

Vicki Lemieux [01:20:44] I would be totally remiss if I didn't name my Blockchain@UBC team, particularly Michelle, who you've been interacting with.

Vicki Lemieux [01:20:53] Michelle Ho, who has so ably helped get this all set up and been in conversation with each of you. Anisha Dhillon, my graduate research assistant who is a student at the School of Information. She's just been so awesome in stepping in, you know, relatively quickly and helping get this organized and helping with some background research to support me. And Chung Lu, who was monitoring the hash tag, who is a postdoctoral researcher in blockchain and health care at Blockchain@UBC and the broader Blockchain@UBC team as well, our industry partners as well as our researchers. So thanks. Thanks to the team.

Vicki Lemieux [01:21:41] And I just wanted to end by saying where do we take this from here?

Vicki Lemieux [01:21:45] You know, it's great to have conversations, but it is really important that these conversations have an impact, that the conversations mean something. So the vision that I have for this is that we recorded this. We will transcribe it and we will share the transcriptions with everyone so that you can edit your particular interventions. If there's anything that you want to change or add as context. And we also want to make this a public record so that we can share all of this knowledge that we've exchanged with each other. We can share it more broadly so that it can inform other conversations that are going on, because this is. Not the only one. And of course, also inform the decisions that our policymakers have to make so that they're aware of some of the ideas, the challenges and the solutions that we've discussed today.

Vicki Lemieux [01:22:48] So I welcome you to use that material however you would like for in your own research and to reach out to one another, to reach out to me, to carry the conversation forward and with your ideas about how we might actually continue this conversation and in more concrete ways as well. So thanks, everyone. It's been fantastic. And I'm just deeply grateful for this moment and to have learned so much from each of you.
So with that, I'm going to end this Zoom-a-thon and wish you all. Good night. Good afternoon. Good morning. Depending on where you are in the world. And so thanks, everyone.
<table>
<thead>
<tr>
<th>Time (all times are Pacific Time)</th>
<th>Lead Witness</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30-9:00</td>
<td>Victoria Lemieux, Opening Remarks and Welcome</td>
</tr>
<tr>
<td>8:45-9:00</td>
<td>Federal Minister for Digital Government, Joyce Murray, Opening Remarks</td>
</tr>
<tr>
<td>9:00 – 9:15AM</td>
<td>Victoria Lemieux, Vote of Thanks to Minister Murray and Review of Q&amp;A Protocol</td>
</tr>
<tr>
<td>9:15 – 9:30AM</td>
<td>Ann Cavoukian</td>
</tr>
<tr>
<td>9:30 – 9:45AM</td>
<td>Lili Liu</td>
</tr>
<tr>
<td>9:45 – 10:00AM</td>
<td>Jennifer Pougnet</td>
</tr>
<tr>
<td>10:00 – 10:15AM</td>
<td>Robin Renwick</td>
</tr>
<tr>
<td>10:15 – 10:30AM</td>
<td>Chandana Unnithan</td>
</tr>
<tr>
<td>10:30 – 10:45AM</td>
<td>Ciara Staunton</td>
</tr>
<tr>
<td>10:45 – 11:00AM</td>
<td>Holly Longstaff</td>
</tr>
<tr>
<td>11:00 – 11:15AM</td>
<td>Yann Joly</td>
</tr>
<tr>
<td>11:15 – 11:30AM</td>
<td>Charles Alessi</td>
</tr>
<tr>
<td>11:30 – 11:45AM</td>
<td>Nadia Diakun</td>
</tr>
<tr>
<td><strong>11:45AM to 12:00PM BREAK</strong></td>
<td></td>
</tr>
<tr>
<td>12:00-12:15</td>
<td>Michael McDonald</td>
</tr>
<tr>
<td>12:15 – 12:30PM</td>
<td>Robert Fraser</td>
</tr>
<tr>
<td>12:30-12:45</td>
<td>Michael Cholod</td>
</tr>
<tr>
<td>12:45 – 1:00PM</td>
<td>Jesse McKee</td>
</tr>
<tr>
<td>1:00-1:15PM</td>
<td>Steve Magennis</td>
</tr>
<tr>
<td>1:15 – 1:30PM</td>
<td>Paola Ardiles</td>
</tr>
<tr>
<td>1:30 – 1:45PM</td>
<td>Nora Weber</td>
</tr>
<tr>
<td>1:45 – 2:00PM (May 6th 5:5:45 – 6AM JST)</td>
<td>Kohei Kurihara</td>
</tr>
<tr>
<td>Time</td>
<td>Speaker</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>2:00-2:15PM</td>
<td>Ma’n H. Zawati</td>
</tr>
<tr>
<td>2:15-2:30PM</td>
<td>Noelannah Neubauer</td>
</tr>
<tr>
<td>2:30 – 2:45PM</td>
<td>Ajit Babu</td>
</tr>
<tr>
<td>2:45-3:00PM</td>
<td>Victoria Lemieux, Vote of Thanks to participants</td>
</tr>
</tbody>
</table>

**This Seminar will close at 3PM PST**
Appendix B – Participant Background Information

The Honourable Joyce Murray P.C., M.P.

The Honourable Joyce Murray was first elected as the Member of Parliament for Vancouver Quadra in 2008. Minister Murray is a dedicated community leader with a deep commitment to environmental sustainability and democratic engagement. Her federal political career follows a 25-year career building an international reforestation company and four years serving in the Cabinet of the Government of British Columbia.

Minister Murray is a thought leader, driving progressive new policies in government. Whether advocating for strong, smart environmental measures such as a tanker ban on British Columbia’s north coast or for the legalization and strict regulation of cannabis, her ability to envision and deliver on bold new ideas comes from her depth of experience in politics and business. Her interest in environmental sustainability was evident in her master’s thesis on global warming, which contributed to her receiving the Simon Fraser University Dean’s Convocation Medal for top MBA graduate of 1992.
Victoria L. Lemieux is an Associate Professor at the University of British Columbia School of Information. Her interests include risk to the availability of trustworthy records, in particular in blockchain record keeping systems, and how these risks impact upon transparency, financial stability, public accountability and human rights. Between 2014-2016, Dr. Lemieux worked with the World Bank on transparency and information management to support economic and social development, leading various big data analytics projects and winning the Bank’s Big Data Innovation Award in 2015. In 2016, Dr. Lemieux founded, Blockchain@UBC’s multidisciplinary blockchain research cluster and in 2019 NSERC awarded her $1.6M to train up to 139 masters and PhD students from multiple disciplines in blockchain and distributed ledger technology over the next five years. Dr. Lemieux has won several awards for her research and contributions to the field of archives and records management.
Lead Witnesses
Charles Alessi

Dr. Charles Alessi is a globally recognized and trusted leader in health care. He brings a wealth of experience, particularly around health systems and the interface between healthcare, social care and the personalization of wellness. He is a physician in London, with more than 40 years of experience in all aspects of clinical practice in the UK National Health Service, also being a past chairman of the National Association of Primary Care. He is the global Chief Clinical Officer of HIMSS, the membership digital not-for-profit organisation, and in this role travels the world assisting governments, large corporations and hospital chains and HIMSS members in the utilisation of data and information to improve the health and wellbeing of citizens. He is also the Senior Advisor to Public Health England, leading thought leadership around productive healthy ageing including dementia, and targeting risk reduction. He has extensive experience in military medicine, being a past Medical Director and Director of Clinical Governance for the British forces in Germany. He holds a variety of international academic positions both in Europe and the Americas and has published widely in the media and journals. He is an Adjunct Research professor in Clinical Neurosciences at the Schulich School of Medicine at the University of Western Ontario, Canada and Visiting Scholar at the Odette School of business in Windsor, Ontario, Canada.
Paola Ardiles is a practitioner scholar based at Simon Fraser University. She has been recognized for her innovative, collaborative and inter-sectoral approaches in health promotion research, policy, practice and education. Paola’s work is rooted in community-engaged scholarship, systems thinking and participatory practice. In 2013, Paola founded Bridge for Health as a local and global self-organized network promoting public engagement and community health. Today she continues to build partnerships and facilitate dialogue to foster the development of practical and creative upstream solutions to tackle complex public health challenges.
Dr. Ajit N Babu, MD, MPH, FACP is Professor of Internal Medicine at Saint Louis University, USA, and a staff physician at the St. Louis VA Medical Center. Dr. Babu is also founder director of the Center for Advancement of Global Health, an NGO based in Cochin, India. He is American Board Certified in both Internal Medicine and Preventive Medicine (Subspecialty Clinical Informatics) and also holds an MPH from Saint Louis University. Dr. Babu was the founder director of the Centre for Digital Health focusing on telehealth and health informatics at the Amrita Institute of Medical Sciences in Cochin, India. He was nominated by the Indian Space Research Organization (ISRO) as an official delegate from India to the United Nations Action Team (AT) 6 dealing with space-based technologies in public health. Dr. Babu is presently on the UN Expert Focal Group on Space and Global Health of the United Nations Office for Outer Space Affairs (UNOOSA), Vienna. He has been a visiting professor teaching telemedicine at the University of Addis Ababa, Ethiopia as arranged by the University of Oslo, Norway. Dr. Babu has also been an invited expert on biomedical informatics for the Indian Council of Medical Research (ICMR). His areas of academic interest include telehealth and applied health technologies in global health.
Dr. Ann Cavoukian is recognized as one of the world’s leading privacy experts. Dr. Cavoukian served an unprecedented three terms as the Information & Privacy Commissioner of Ontario, Canada. There she created Privacy by Design, a framework that seeks to proactively embed privacy into the design specifications of information technologies, networked infrastructure and business practices, thereby achieving the strongest protection possible. In 2010, International Privacy Regulators unanimously passed a Resolution recognizing Privacy by Design as an International Standard. Since then, PbD has been translated into 40 languages! In 2018, PbD was included in a sweeping new law in the EU: the General Data Protection Regulation.

Dr. Cavoukian is now the Executive Director of the Global Privacy & Security by Design Centre. She is also a Senior Fellow of the Ted Rogers Leadership Centre at Ryerson University, and a Faculty Fellow of the Center for Law, Science & Innovation at the Sandra Day O’Connor College of Law at Arizona State University.
Michael Cholod, CEO of Peer Social has grown up alongside video games, personal computers and the Internet. With over 20 years experience in Entrepreneurship, Sales and Marketing and Venture Capital, I have witnessed the explosive growth of some of the world’s most revolutionary technologies and watched the Internet transform the world.

The Internet had the potential to be a positive tool, one that could unite us—instead it is being used to steal our data, divide us, and spread mis-information. This is why I am committed to creating a user-centric solution to counteract a serious problem—cloud based, social networking and the Surveillance Capital business model.

We founded Peer Social to pursue technological innovation with a conscience—a place where the best and brightest minds can work together and build something that will have a positive impact on the world. Our team is made up of dedicated decentralists and blockchain enthusiasts who are researching and developing new Internet architectures and technologies, in an effort to solve some of the most pressing problems of our time.

Our focus is on distributed ledger, decentralised computing and adaptive mesh networking. These technologies have the potential to produce a sustainable foundation for a new, distributed Internet—an Internet where everyone can feel safe, secure, and in control of their data and their digital identity.
Nadia Diakun-Thibault is CEO and Founder of PanSophX Inc., a consultancy firm advising on cybersecurity, cyber resilience, and blockchain; and CEO of PharmOrchard, which is developing a secure environment for the storage and analysis of healthcare information by using blockchain technology as an effective solution to address the privacy and security concerns of the stakeholders. She held an Order-in-Council appointment, Province of Ontario Commissioner with the Ontario Advocacy Commission. Her federal government experience spans security intelligence, innovation, and public policy. In 2016, co-authored a paper entitled *Blockchain and Health IT: Algorithms, Privacy and Data* which was ranked first among the 15 finalists of the ONC HealthIT Blockchain Challenge 2016.
Dr. Robert Fraser is the President and CEO of Molecular You, a digital health company utilizing integrated biomarker analyses to deliver personalized health insights and action plans. As a co-founder of The Personalized Medicine Initiative (PMI), Dr. Fraser has been at the forefront of developing the framework and technologies to bring personalized medicine into healthcare practice. Backed by his expertise in molecular diagnostics, molecularly-targeted drug discovery and development, biochemistry and regulatory compliance, Dr. Fraser has been a leader in the implementation of personalized care in Canada. He has also been involved in leading drug discovery and development projects at Sanofi, Xenon, Neuromed and CDRD. Dr. Fraser received extensive training in the molecular mechanisms of endocrinology while completing his Ph.D. at the University of Alberta and Harvard Medical School and Post-Doctoral Fellowships at Hospital for Sick Children, Toronto and IGBMC, Strasbourg France. In addition to Dr. Fraser’s scientific accomplishments, he has been involved in the raising of more than $37M in funding. Dr. Fraser is also co-founder of GenXys Health Care Systems, Personalized Biomarkers Incorporated.
Yann Joly, Ph.D. (DCL), FCAHS, Ad.E. is the Research Director of the Centre of Genomics and Policy (CGP). He is an Associate Professor at the Faculty of Medicine, Department of Human Genetics cross-appointed at the Bioethics Unit, at McGill University. He was named advocatus emeritus by the Quebec Bar in 2012 and Fellow of the Canadian Academy of Health Sciences in 2017.

Prof. Joly is a member of the Canadian Commission for UNESCO (CCU) Sectoral Commission for Natural, Social and Human Sciences. He is the current Chair of the Bioethics Workgroup of the International Human Epigenome Consortium (IHEC) and Co-Lead the regulatory and ethics work stream of the Global Alliance for Genomics and Health (GA4GH). He was Chair (2017-2019) of the Ethics and Governance Committee of the International Cancer Genome Consortium (ICGC). He is also a member of the Human Genome Organization (HUGO) Committee on Ethics, Law and Society (CELS).

Prof. Joly’s research interests lie at the interface of the fields of scientific knowledge, health law (biotechnology and other emerging health technologies) and bioethics. He created the first international genetic discrimination observatory (GDO https://gdo.global/en/gdo-description) in 2018. He has published his findings in over 150 peer-reviewed articles featured in top legal, ethical and scientific journals. He served as a legal advisor on multiple research ethics committees in the public and private sectors. Prof. Joly also sits on editorial committees and acts as a reviewer for a wide range of publications in his field. In 2012, he received the Quebec Bar Award of Merit (Innovation) for his work on the right to privacy in the biomedical field.
Kohei Kurihara is Chief Marketing Officer at CollaboGate, and President of Tokyo Chapter, Government Blockchain Association. Kohei has several experiences at blockchain spaces, and leading local community such as Government Blockchain Association in Tokyo. At CollaboGate, provide the blockchain ID authentication service based on privacy orientation. And he has established privacy by design working group practices which is democratic community for privacy based data society.
Lili Liu is Professor and Dean of Applied Health Sciences at the University of Waterloo. She earned her BSc in Occupational Therapy and MSc and PhD in Rehabilitation Science at McGill University. She is an AGE-WELL network investigator. Her research examines user adoption and acceptance of technologies by older adults and their care partners to maintain one’s ability to live in the community. She is conducting national research projects with persons living with dementia on topics such as digital storytelling, and strategies to mitigate risks of going missing.
Holly Longstaff is the Director of Privacy and Access at PHSA Research and New Initiatives, Provincial Health Services Authority. Holly is responsible for guiding the development, recommendation and implementation of innovative approaches to privacy policy and practice to build accountable information stewardship and privacy conscious practices that enable the execution of PHSA’s expanded mandate and the conduct of health research. She advises on the privacy requirements relating to new and expanded provincial initiatives working closely with PHSA’s Information, Access and Privacy, and Legal Services teams. She also provides leadership in developing and implementing governance mechanisms to enable nimble, multidisciplinary review of privacy and security requirements for new and expanded initiatives and research, including province-wide platforms and systems, digital and information technologies, and data access/sharing. Holly is a PhD level trained ethicist and research consultant. She serves as the ethicist on the BC Cancer Research Ethics Board and a US-based IRB. She has worked as a consultant for Health Canada, the Public Health Agency of Canada, and the CIHR Ethics Office and her work has been published in a variety of journals including CMAJ, Trends in Neurosciences and Cell Stem Cell.
Steve Magennis, former Senior Director at Avanade is a skilled technology executive and leader who has been at the forefront of cloud, AI, and digital transformation at Microsoft, Accenture and Fortune 100 clients throughout his career. He is deeply connected to the evolution of decentralized architectures and the advancement of cryptographic identity that is changing the way enterprises and governments approach entrenched business and social problems.
Dr. Michael McDonald was the founding Director of the W. Maurice Young Centre for Applied Ethics in the School of Population and Public Health at the University of British Columbia and the occupant of the first endowed chair in applied ethics in Canada. His academic career began over 50 years ago at the University of Waterloo where his work centred on moral and political philosophy. There he developed the strategic vision for advancing interdisciplinary applied ethics research across Canada that was adopted by SSHRC. For the past 25 years, McDonald has focussed on the ethical conduct of research involving humans and played a leading part in the creation of the Canadian national standard in this area. He has been a PI on numerous CIHR sponsored research projects. McDonald's research has been supported by a number of public, private, and professional agencies and organizations. He takes great satisfaction in the many accomplishments of the colleagues, students and organizations that he has assisted over his career.
Jesse McKee is the Head of Strategy at 221A. He leads the Organization’s advancement, communications, research, and programming. From 2019-22, he is the lead investigator on 221A’s Blockchains & Cultural Padlocks Research Initiative. Previously, he was the Curator of Walter Phillips Gallery, The Banff Centre and the Exhibitions Curator, Western Front, Vancouver. In 2017, he was the co-curator, with Daina Augaitis, of Vancouver Special: Ambivalent Pleasures, the inaugural edition of a civic triennial exhibition at the Vancouver Art Gallery. As a curatorial resident, he has worked with Things that can happen, Hong Kong and Tranzit.org, Romania. McKee served as a juror for the Sobey Art Award and was a member of the Canada Council for the Art’s Asia Pacific Delegation. He has written essays and reviews for Canadian Art, C Magazine, Fillip, Border Crossings, Kaleidoscope, and Cura. His recent catalogue essay, Surreal Ghosts and Neuroplastic Ancestors correlates Julia Feyrer and Tamara Henderson’s filmmaking with the neuroplastic effects of Vancouver’s economic enclosure over the past decade; published by the Morris and Helen Belkin Art Gallery, University of British Columbia and Institute for Contemporary Art, University of Pennsylvania.
Noelannah Neubauer is a Postdoctoral Fellow in the Faculty of Applied Health Sciences at the University of Waterloo and is an MScOT student at the University of Alberta. She earned her BHK and MSc in Human Kinetics at UBC Okanagan, and her PhD in Rehabilitation Science at the University of Alberta. She is affiliated with AGE-WELL, and is the co-founder of the International Consortium on Dementia and Wayfinding. Her present research examines approaches to mitigate the risks of going missing, and the application of self-sovereign identity among missing persons data.
Jennifer Pougnet currently serves as the Data Policy Strategy Leader for the Personalised Healthcare Center of Excellence at Roche in Basel Switzerland. She has an eclectic background working predominantly in the public sector in Canada; implementing Electronic Medical Records in large health systems, developing and implementing both operational and legislative policy as part of a health system and in Ministerial Offices. She has worked in Clinical Information Systems, Infection Prevention & Control and Quality & Medical Affairs programs in these capacities. With Roche she has also worked on Companion Diagnostic and Next Generation Sequencing access as well as Precision Medicine policy identifying and navigating innovative funding pathways.

In her free time Jennifer has volunteered with the Canadian College of Health Leaders; serving on their conference program advisories, Certified Healthcare Executive curriculum development committee and delivering social media campaigns. She also has worked extensively with Emerging Health Leaders serving as both a Local Node and a National Co-Chair with the organisation.
Robin Renwick

Robin currently forms part of the Applied Research & Innovation team at Trilateral Research. He is the research lead for Trilateral on the European Commission H2020 project SOTER, which is tasked with developing a biometric identification and authentication digital on-boarding platform for the financial services sector. Trilateral leads the privacy, data protection, and ethical impact assessments, as well as the security risk assessment. Robin has developed an interdisciplinary research background; concerned mostly with the triumvirate of networks, technology, and society. His most recent research focused on the interface between privacy and blockchain technology; a boundary theory-based study of varied perspectives as told by active participants in the blockchain ecosystem. He is a member of the ISO/TC 307 blockchain and distributed ledger technologies standardisation efforts, and a member of CEN/CLC JTC 19 – Identity Management. Robin holds a PhD from Queen’s University Belfast.
Dr Ciara Staunton is a Senior Lecturer in Law at Middlesex University (London) and a Senior Researcher at the Institute for Biomedicine, Eurac Research (Italy). In addition she is an Honorary Research Associate at the Faculty of Health Sciences, University of Cape Town and a Consultant to the South African National Health Laboratory Service. Her research focuses on the governance of new and emerging technologies, in particular stem cell research, genomic research and biobanking. Ciara’s current research focuses on the sharing of health data for research, with a particular focus on Africa. She has been in receipt of grants from the Wellcome Trust, the National Institutes of Health (NIH) and the Irish Research Council and has been involved in the development of policy in Ireland, Bahrain and Africa.

From 2010-2013 she was a post-doctorate researcher at the Centre for Medical Ethics and Law, Stellenbosch University. During this time she co-ordinated the Advancing Research Ethics in Southern Africa (ARESA) Program and was a member of the H3Africa Ethics and Regulatory Issues Working Group. She obtained her PhD from NUI, Galway for her thesis The Regulation of Stem Cell Research in Ireland.

Prior to starting her academic career, she was a Legal Researcher at the Law Reform Commission of Ireland.
Dr Chandana Unnithan (PhD, MbusComputing, MBA) is a professor in applied public health informatics from Torrens University Australia; and represents Australia in the United Nations COPUOS as a digital health expert. She is also a member of Space and Global Health Expert group of the UNOOSA and an appointed expert in the WHO Digital Health Group. She is on the medical research advisory board of Rapid Response Revival, an Australian firm that has developed the smallest defibrillator for mobile phones. In Canada, she is currently CTO/CIO for Lifeguard Digital Health, a digital health company that has built a pioneering application for supporting emergency services during the opioid crisis, and is in the process of developing multiple public health crises management applications. She is also on the advisory committee of MyPdx - a project from Canada’s Digital Technology Supercluster, aimed at building a novel blockchain solution that leverages the open source blockchain framework, to enable privacy preserving and secure sharing of personal health data.

Her expertise in digital health (encompassing IoT, AI, Health Informatics, geo-spatial/remote sensing technologies, blockchain in health) was established over 15+ years in pioneering/implementing innovative technological solutions in large public hospitals in Australia, while and also being a professor in applied public health informatics. She is extensively published with over 100 peer reviewed scientific papers and is an invited keynote speaker/panelist at international conferences in Australia, Canada, USA and Europe.
Nora Weber is communications specialist with a global perspective and a solution orientation. Believing that each of us can make a difference, she works in the areas of social justice, conservation, and culture.

As a world citizen first, she sees culture as the soul of a country and seeks to celebrate our inclusive history and our diversity as the strength of our nation. It is her strong belief that the world is a global village. People long to connect with each other and the best way to facilitate that is through stories that celebrate our shared journey.
Ma’n H. Zawati (LL.B., LL.M., Ph.D. (DCL)) is an Assistant Professor at McGill University’s Faculty of Medicine and the Executive Director of the Centre of Genomics and Policy in the Department of Human Genetics. He is also an Associate Member of McGill’s Biomedical Ethics Unit. His research concentrates on the legal, ethical and policy dimensions of health research and clinical care, with a special focus on biobanking, data sharing, professional liability, and the use of novel technologies (e.g. mhealth apps, WGS, WES) in both the clinical and research settings. Dr. Zawati is funded by Genome Canada, Genome Quebec and the Terry Fox Research Institute. His work is interdisciplinary, drawing together perspectives from law, ethics, bioinformatics, genomics, and policy. He’s also a frequent presenter on a variety of the most critical and topical issues in healthcare and the biosciences. He has appeared at 100+ international conferences, symposia, meetings, and has shared his expertise with universities, research ethics boards and law firms. Dr. Zawati has published 13 book chapters and 45+ peer reviewed articles in leading publications such as Nature Reviews Genetics, the Canadian Medical Association Journal, the Journal of Law and the Biosciences, the Journal of Medical Genetics, and the McGill Journal of Law and Health. In 2015, he was awarded the Queen Elizabeth II Diamond Jubilee Scholarship (stay at Oxford University) and was named a Royal Society of Canada Delegate for the IAP Young Scientists of the Year international symposium. In 2014, the Young Bar Association of Montreal named him as one of its Lawyers of the Year.