**August 10, 2021 Meeting - Seattle Community Technology Advisory Board**

Topics covered included: Jim Loter, Interim CTO; Law and Cybersecurity with Prof. Ryan Calo; Committee Updates

**This meeting was held:** August 10, 2021; 6:00-7:45 p.m., via Webex

**Attending:  (All via Webex)**

**Board Members:** Rene Peters, Camille Malonzo, Nicole Espy, Femi Adebayo, Brandon Lindsey, Lassana Magassa

**Public:** Prof. Ryan Calo,Dorene Cornwell, Eryk Waligora, Laura Loe, Harte Daniels, Coleman Entringer, Andy Katz, Jackson Brown, Resident, Mathew Trummel, Mitchell Harper

**Staff:** Jim Loter, Trayce Cantrell, Greg Smith, Cara Vallier, David Keyes, Vicky Yuki, Vinh Tang, Tom VanBuren (SPU), Aurilee Gamboa, Cass Magnuski

**28 In Attendance**

**Rene Peters:**   Welcome to the August edition of CTAB. Just as a note, you saw the recording start. We're just doing that for the purpose of the minutes. We will publish the text transcripts on our web site, but there won't be an audio recording of the meeting. I wanted to start off the same way we start off every month, with a quick acknowledgement that we are on the traditional land of the first people of Seattle, the Duwamish people, and give honor to them past and present and gratitude for the land, itself and the Duwamish Tribe.

Once again, thank you everybody, for giving us some of your beautiful, pre-secondary heat wave here in Seattle. It's good to see everybody's faces again. Oddly enough, since July, when we last talked, it has been a relatively quiet month. When I was searching around for my random tech tidbit to chat about, there are couple of interesting stories floating around and getting more traction, really centering around this tension between data privacy and personal ownership. One that you may have seen in the news recently centered around what is called Section 230, which is a part of the US Communications Decency Act. Essentially, it states that no provider or user of any interactive computer service will be responsible as the publisher or speaker of any of the information that is transmitted by another content provider. In practice, what that really means is that service providers aren't -- it sort of protects service providers, themselves, from being liable from the material that users of that service post. This has popped up in a few different places, such as Facebook, such as the QAnon, 4chan and 8chan. Most recently, two of the Democratic senators, including Amy Klobuchar, they introduced what they're calling the Health Misinformation Act. That happened in mid-July, a week or so after we met. And it is really aimed at tamping down on any misinformation that involves Covid and any ongoing health crises on some of these large platforms. Interestingly enough, Biden has weighed in on this, saying that disinformation on social media is effectively killing people. So, there are some really interesting definitional questions and issues that are being discussed. One of them is the fact that the bill, itself, has been introduced and written and only is aimed at information that has been "algorithmically amplified" on these platforms, and so where do you draw the line there, as far as information that is recommended versus ads that are amplified through more official platforms that are purchased. So, there are a couple of interesting definitions that are developing there, but here is a link to a summary article on the early moving parts. This discussion is working its way into the mainstream. <https://gizmodo.com/senators-put-section-230-in-the-crosshairs-in-battle-ov-1847344879>

Another more really recent discussion that's probably bubbling up centers on Apple devices. You may have heard that they're rolling out in the near future a technology that actually stands the Apple cloud and specifically image files for harmful media regarding children. It's a pretty clear ethical tug of war on creating a benefit in the form of safety for very vulnerable populations of children. But then, also, the larger questions of ownership of private data and if there's a slippery slope, not just in this country but in other countries. There is worry that other legal systems or government entities may take advantage of the access and surveillance of the Apple cloud. So, that's another really fascinating discussion that I think might have popped up within the last couple of weeks. I think that one is in the very, very early stages. Now, Apple -- they have the reputation of being very, very hardline whenever governments try to get involved. So, they're maintaining that line right now. But a lot of data privacy activists and other folks in the field seem to be a little bit worried. So, that's another really fascinating discussion to look out for.

That's my random tidbits. Both of those topics target very interesting questions on the relationship between what is private and what do you rally own as far as the data on the platforms that you use. With that, I want to start introductions. We have a special guest here today that I wanted to actually start off with before we start reading down the list. We have Jim Loter here, who is the interim CTO for the City of Seattle. And I just wanted to give him the stage and the platform to introduce himself to us. For those of the attendees who have been at some of our past meetings, you will know that the relationship between this board and the CTO is very important as far as having a stakeholder and key lynchpin within the City as far as driving on the agenda, technology used in the City, and information technology and how we improve and learn from it. So, Jim, I wanted to start off by actually giving you the floor, and giving you whatever amount of time you wanted. Tell us about yourself, and your experiences up to now, and maybe some of what you have in store. So, welcome and thanks for showing up.

**JIM LOTER, INTERIM CITY OF SEATTLE CHIEF TECHNOLOGY OFFICER**

**Jim Loter:**   Thanks, Rene, for having me tonight. I appreciate being invited. I'm Jim Loter. I've been working with Seattle IT now for over five years in various roles. Some of you already know me. I was a fairly regular attendee at CTAB meetings back in the day. My first job with the City was as director of digital engagement, which included the Community Technology group, with which you are very well familiar. They have been the steward and liaisons to this board pretty much since its inception, I think, at least involved in some capacity with CTAB. And that area also included our privacy program. I was responsible for the privacy program when the City's Surveillance Ordinance was passed, and had the pleasure of working through the the early year, year and a half or so of implementing and executing on that piece of legislation, and fulfilling the responsibilities and the duties that it describes for Seattle IT to pay. So, I appreciate the tech tidbits. Those are exactly the issues that I'm paying attention to in the media, as well. And, certainly, privacy and matters of how the City interacts with and protects the public's data, and the technology that we implement, and then have an effect on areas of great concern to me. I take that responsibility very seriously.

Back in 2019, I was moved into a more operational role, overseeing what we called frontline services at the time. So, my involvement with those activities as I delved into improving the services that we owe to our internal clients in the City. I have been doing a variation of that role for the last couple of years. So, I'm very honored and excited to be appointed by the Mayor as the interim technology officer. She has made it clear that she is not going to make a permanent decision on this role. So, the fate of this role is in the hands of whoever wins the election in November. So, we will see what that brings us.

But I've got a little bit of time here to make a difference, and to work with the executive team and the path of the department to influence some very exciting things. Chief among those, I think, in the cybersecurity space, includes the completion of our rollout of (unintelligible) authentication throughout the City, our rollout of mobile device management, which allows us to implement security and configuration settings on mobile devices throughout the City. We are also rolling out data loss prevention as a program to scan the City's incoming and outgoing communications for sensitive information that we don't necessarily want leaked in plain text format. So there are a number of things. Our chief information security officer and director of security infrastructure, Greg Smith, is here today. And he is involved in those efforts. And we are working on a number of things with our partners over in City Council. I think you're familiar with Internet for All work, as well as the work of surveillance technology and our work on documenting and reviewing surveillance technologies to make sure that they are compliant with the ordinance and with best practices. We are also in the middle of finalizing our report on our Race and Social Justice impacts and initiatives from the past year, which we will also be sharing with our Council committee and work with City Council.

So, there's a lot going on. I thin our main focus that's in the background of all of this is how the City's return to office activities are proceeding. We had a role in bringing our staff back to the office in a safe and secure way, as well as supporting the staff in other City departments that are increasingly working out of the office, or in some sort of a hybrid capacity. So, as you can imagine, with 13,000 City employees, that's a pretty large logistical problem. How we deliver our services in Seattle IT, now and in the future, is very dependent on how all of that metes out.  As you know, the news changes almost on a day to day basis with information that is affecting the timing and peoples' dispositions towards that exercise. So, it's been very challenging. It's been challenging for our staff to not know on a day to day basis what is necessarily happening when. Obviously, people's opinions and feelings about it change, based on that information, too. So, that's just a bear present in the background, causing some stress, causing some anxiety. But we have a really good team working on that and providing some great resources for our staff to handle that transition.

So, that's basically me, and what I'm looking forward to in my 60/120/180-day outlook for however long I am here in this role. I'm happy to take any questions. I know you've got a packed agenda. I will turn it back over to you.

**Rene Peters:**   Sure. Absolutely. Let's see, what do we have? 6:18 here? Actually, I will move on to the rest of the introductions, and then I want to make sure that we are respectful of Prof. Ryan Calo's time. He is slated to get started here at 6:25. So, I'll actually get back to you, Jim, if you are able to stay until after that session, we can get back to you with some questions and answers.

**Jim Loter:**   I am here for the meeting.

**Rene Peters:**   Thank you so much. So, let's continue to go down the list. I will essentially just read down the attendance, and if you can give your name, and if you want to share your affiliation and the area of Seattle that you're calling in from, that would be excellent.

**INTRODUCTIONS**

**Rene Peters:**   All right. So that's it for introductions. So glad to see everybody's faces. Next, since we do have quorum with our board members, I wanted to very quickly take care of some business items. That is approving the minutes from July and approving this agenda. The minutes from July were posted as linked with the agenda for August that was sent out this week. It included our Technology Matching Fund feature of the Multimedia Resource and Training Institute, and also an announcement on supplemental awards for the Technology Matching Fund. If I can get a motion from the board to approve those minutes?

**Femi Adebayo:**  I move to approve the minutes.

**Brandon Lindsey:**  Second.

**Rene Peters:**   And you read my mind. Thank you, Brandon, for the second. Can I have the 'ayes?' Are there any 'nays' or abstentions? All right. That will pass to approve the July minutes. Now I'd like to get a motion to approve the August agenda.

**Femi Adebayo:**  I move to approve.

**Rene Peters:**   You're on fire. Thank you, Femi. Is there a second for Femi?

**Nicole Espy:**   Second.

**Rene Peters:**   Thank you, Nicole. Can I have the 'ayes?' Any 'nays' or abstentions? Excellent. That will pass. Thank you for that, board members. We can move on in our agenda. We are so excited to have Prof. Calo here. He's going to give us a great talk about law and cybersecurity. But, I wanted to hand off to Camille Malonzo and Nicole Espy to introduce him, since the Cybersecurity Committee did such a great job in bringing him in. I'll hand it over to you.

**Nicole Espy:**   Yes. I'll keep it short. Prof. Calo is a professor at the University of Washington School of Law, and a founding co-director of the interdisciplinary UW Tech Policy Lab and the UW Center for an Informed Public. We are really interested in learning more about the interaction between law and cybersecurity. We got a great recommendation to speak with Prof. Calo, and to learn a little bit more about what he will go much in depth with today, which is the relationship between the law around hacking, and what is currently unfolding with AI and machine learning. We appreciate the talk. Thank you.

**LAW AND CYBERSECURITY**

**Prof. Ryan Calo:**   First of all, it's really lovely to be able to address you all. I've had such productive interactions with some of you in the past. Notably, Jan Whittington and I did a comprehensive review of Seattle's open municipal data project initiative. And I have interacted with many of you through that process. So, Jan is a professor in the College of Built Environments, and she and I did work together just looking comprehensively at Seattle's open municipal data. And making a series of recommendations, almost all of which were adopted by the City. The City was incredibly open and made available documents and people so we could really do a thorough job. And, ultimately, the City got an award from a prominent think tank for best practice in open municipal data. So, I thought that was a wonderful partnership between us, and I still think of it often.

I am a law professor at the University of Washington, and I hold courtesy appointments in computer science and information science along with Tadayoshi Kohno and Batya Friedman. Batya is an information scientist and a pioneer of a method called value sensitive design. And Tadayoshi is a computer security researcher. For example, he is appointed to the Air Force Security Task Force. We founded this thing called the Tech Policy Lab. And one of your board members, Lassana Magassa, is a post-doc at the lab. And the mission of the lab is to help policy makers like yourselves, broadly defined, but certainly evolved easily within our definition, make wiser, more inclusive tech policy. And the way we work is we tackle individual questions about, for example, what is best practice in open municipal data, what are the law and policy implications of augmented reality. But we also tackle eco-system-wide questions, like how do we introduce more diverse perspectives into tech policy, which tends, usually, to reflect the mainstream. So, we're thinking both about the macro and the micro both in individual technologies and context, like the City using augmented reality and also broader issues around the tech policy eco-system.

In addition to that work, I co-founded and am a PI, a primary investigator, for the Center for an Informed Public. That organization is about a $10 million research organization that works specifically on misinformation and disinformation. And my primary goal in addressing you tonight is just to mention that we are a resource here for you. Whether it's the Tech Policy Lab or it's the Center for Informed Public, our *raison d'etre* is to help folks like you make policy decisions that are wise and in the public interest. We do that through research. We put people in teams. And that's just what we do. And so the remarks I'm about to make about a specific project are really just by way of illustration. This is the kind of thing we're up to. This is the kind of thing we do, we feel, well. But really, I want to just tell you that we are a resource for you all.

The specific work I want to mention actually comes out of the Tech Policy Lab. As is typical of the lab, we decided to tackle a very difficult emerging question of technology policy that requires the construction and integration of the interdisciplinary team. And the specific question we are looking at is how does the increased prevalence of machine learning AI models and decision-making, how does that affect the cybersecurity picture, and most specifically the definition of hacking.

The definition of hacking has been one of those things that has been pretty consistent and pretty resilient since the 1980s. The federal definition of hacking comes out of War Games. I'm sure most of you are familiar with the Matthew Broderick vehicle, War Games, right? This is like, would you like to play a game. This hapless, super smart teenager ends up hacking into a nuclear facility and ends up almost starting a nuclear war. It really scared a lot of folks in the 1980s. The Reagan Administration ends up recommending to Congress that Congress ultimately pass what is called the Computer Fraud and Abuse Act, and it has this definition of hacking, which is this classic definition of hacking under a federal law which says that what you're doing is you are breaking into a computer. You're bypassing security protocol in order to access the contents of the computer. And you're exfiltrating data where you're messing around in there, or you're making it unusable. These are the classic things that you do with hacking. It's the kind of thing that, of course, all of you deal with in your daily jobs. And it worked out really well for a long time. This was the 1980s. The definition has been construed and evolved through the court, or whatever. You are exceeding authorization, or you are engaged especially in unauthorized access. And that has been defined by the courts as bypassing the security protocol. Not only has this been the (unintelligible) for hacking in the United States, but it's also the international definition of hacking, as well as the definition of hacking in any number of different contexts. And importantly, when we have expectations of a company, that it have adequate cybersecurity, what we have in mind once again is the idea that you can stop it, that it can't be too easy to bypass your security protocols if you have a huge company, and you touch lots of consumers, lots of citizens. If it's too easy to get by security protocols, if you have some admin password that's 1-2-3-4, you're going to find yourself on the other side of a Federal Trade Commission complaint, a state attorney general, whatever it might be. So, both our definition of hacking for purpose of federal criminal and civil law and our expectations around adequate security for consumer protection are pegged to this definition of security breach.

Enter a machine that's running artificial intelligence. For a time, the most focus was on the ability of artificial intelligence and machine learning -- what is artificial intelligence? It's a set of techniques aimed at approximating some aspect of human or animal cognition using machines. It's not a one thing. It's not an artifact. It's not even a system that could train systems. It's a set of techniques. Machine learning is a particular technique with artificial intelligence in which you train a model on a data set, and then you introduce something, a data set, or a new piece of information, and you get the model to see if it can do a classification, on essentially what amounts to pattern recognition. You train a model on flowers. You show the model something that it has never seen before. You ask it if it is a flower or not, or is it a dog or a wolf. That's again another set of techniques within the broader techniques of artificial intelligence. But, as you might imagine, it's sort of taking a lot of things over. We see more and more instances of artificial intelligence and a subset of machine learning doing translation, making decisions of consequence for people, navigating drones, navigating driverless cars, and so on.

So, our contention as a team at the Tech Policy Lab was that too much of an adequate focus on the ability to use AI in order to both attack systems and to defend them. And so there have been challenges and there has been a lot of tension. How do you use artificial intelligence to scan the network and see the vulnerability. How do you break in? How do you bypass security protocol using artificial intelligence? And also, how do you use artificial intelligence to spot a pattern that might be indicative of malicious activity? How do you use AI to protect yourself? How do you use AI to attack a network? So, it has been a sword and shield approach. Even as this conversation is unfolding, you have a bunch of clever researchers who are in computer science and elsewhere, trying to show how a system that is engaged in classification and detection is vulnerable? It's smart, but it's too smart. It's clever. it's too clever, right? The idea is once you are deploying a system in the world that is using a model to make decisions about that world to identify something to decide what speed you should be going, whatever it happens to be, wherever you use that system, all of a sudden you have this model that has been released, and that model ought to do the right thing, but actually might not. And it turns out the more you know about the model, the more you can manipulate these smart systems to do what you want, rather than how they are intended. And this is a set of techniques and a set of really a kind of sub-domain security research that is known as adversarial machine learning. The idea that you could take a trained model and you can trick it. You can get it to do something that it's not intended to do. For example -- I'll give you three.

My colleagues at the university of Washington, including my collaborators for this paper, showed that you could suddenly perturb a stop sign with a sticker in a way that we would notice as people. We'd just see a sticker. Because the car, an autonomous vehicle, can misperceive a stop sign as a speed sign. Researchers at Ten Cent Research showed that you could also cause a Tesla to veer off course, just by putting stickers on the road in the right pattern because the system is constantly looking at the road trying to figure out what is the divider line, what lines it is supposed to stay within, and you can suddenly manipulate that and cause it to drive into traffic. Okay? Another set of researchers, for a third example not involving cars, is researchers at Berkeley showed that if you have a system that is like Amazon Echo, that is waiting for you to give commands, and is usually machine learning to do voice recognition and hear commands, you can play subtle tones that people wouldn't recognize, that cause the system to perceive that you're ordering a specific thing on Amazon. In other words, I can be playing those tones in the background now, and if you don't have headphones on, and unbeknownst to you, your Echo in the background could be making an order on your behalf to Amazon, these Berkeley researchers show.

This is a set of techniques call, again, adversarial machine learning. They come in essentially three different flavors. One of them is when you actually, affirmatively cause a system to -- you figure out a system and you figure out (unintelligible) and you cause it to behave in a way that it's not intended. The second way is you poison a system as it's being trained. So, as consequential decisions are made about us on the basis of machine learning, what you do is you introduce poisonous training data so that when something comes up, you look like you're a great credit risk, but somebody you don't want to be getting a loan looks like a terrible credit risk. An example of this was the way that people poisoned Microsoft K, the chat bot that Microsoft created to work on Twitter that became a misogynist-spewing bot very rapidly. That was through machine learning where people figured out that they could figure out with K in such a way that would poison the model and cause it to behave in a way that they anticipated. And the third thing is that if you really have access to a model and you can query over and over again, you can actually reconstruct the trainings that went into the model itself. You can exfiltrate data in a way that's really surprising. So, you train up a model and it's a model based on data, and you think at that point that the data has become the model and you can't get the underlying data it was trained on. Certainly, you can't get access to the database itself, but it turns out that by clever query, you can reconstruct some or all of the underlying training data.

So, as is typical at our policy lab, we put together a group that consisted of, number one, a person who works deeply in computer security; number two, a person working deeply in computer science specifically on machine learning; and number three, a person who works in law, specifically on privacy law.. We put together a team -- it's actually five of us, so there's a little duplication, but we had all three in these expertises, and we wrote this paper that is called Tricking a Robot on Hacking. What becomes really interesting about adversarial machine learning is it does not seem to line up very well with standard definitions of security problems of hacking. Because, in essence, you're not bypassing security protocol. You are merely deceiving the system into behaving the way that you want. And so it creates this puzzle, which is -- gosh -- is it really not a Computer Fraud and Abuse Act not a problem for you to trick a bunch of driverless cars into perceiving a stop sign as a speed sign? And I understand that you could throw something over a sign or chop down a speed sign. But these kinds of things mean that you could do something at scale. You could really cause havoc at scale and that would be unreachable under federal law. Is it really okay to get on an Echo to buy stuff that people didn't mean to do? Isn't that really a problem?

if you are unconvinced by that and think it could be handled by another law, another idea is is it adequate security if you build a system like that, and it is so easily tricked? Right? Are we okay with building a car that could be so easily fooled into deviating into the wrong lane? Or into speeding up when it sees a stop sign? Or into letting random people buy stuff? Is it adequate security?

You have to ask questions like that. I don't know that I feel comfortable saying that a system is adequately secure when it is so easily fooled by people, even though what is happening is you're not bypassing the security protocol and therefore it doesn't meet the technical definition of hacking.

On the other hand, if we just want to say, you know what, Ryan you're right. Let's just expand the definition of hacking, and it will be also tricking, and we'll just fool systems, and any time that happens, it will be a Computer Fraud and Abuse Act problem, well, then you run into other issues. So, for example, under the Computer Fraud and Abuse Act, government computers get special treatment. And if you hack a government computer, even if you don't do any harm, you can get into a lot of trouble. So, let's say that you show up to an airport, and you're wearing makeup. And the purpose of the makeup is to thwart facial recognition because you don't want to be recognized by the system, so you wear this makeup. All of a sudden, is that a Computer Fraud and Abuse Act -- are you hacking a computer? Because you're tricking it? Ultimately, the purpose of the paper is academic. It's not necessarily to perfectly resolve this question, but it is to tee up the kinds of questions that are arising at the intersection of cybersecurity and law, and then, ultimately, AI machine learning. And to make a point that the problem is broader than just that AI will make it easier to hack, but also easier to defend your systems.

What relevance might this have to you? Well, if you procure software, and the software relies on machine learning, or relies on AI models, one of the things you're going to want to figure out is how resilient is it against manipulation and attack? You might be satisfied with the level of security that they're showing. That they have physical security and encryption, and whatever else you're looking for -- whatever standard you think is met. And yet it could be tremendously easy to manipulate because it is easy to understand the underlying model.

I'll just end there, just to say that we're doing something that we think we are uniquely positioned to do, which is to bring people from very different disciplines, throw them together as a team, integrate our insights, and then provide knowledge to the world in a way that we hope is impartial because we don't have a profit motivation, and so on. And again, we are here to be a resource to folks just like you. If you have any questions, I'd like to hear them. Otherwise, I just appreciate the opportunity to address this group.

**Rene Peters:**   A very, very interesting discussion. Awesome. I think it was just a robust introduction to the problem itself. They bring up these problems from so many different directions. There are just so many permutations of the ways that we can look at it. I was so fascinated, first off. When did you complete and publish that paper. And then, who have been some of your stakeholders? Who consumes that research, and what are the kinds of things that they've gone on to do with it?

**Prof. Ryan Calo:**   That's a great question, and often with tech policy projects, we can point to specific impacts. In this case, this tricking robot hacking paper is just, I think, from last year. It came out in the Berkeley Technology Law Journal. But already, before the pandemic, and before publication, I spoke to the Aspen Cybersecurity Forum in Berlin just basically talking about the need to update this stuff. We've had conversations with intelligence agencies and stuff like that. And then, often I'm called upon to give advice to state and federal law makers and often will mention this issue. It's also been taken up in the popular press. I think though that it is one of the challenges with emerging technologies is, and I'm quoting from my colleague, Tadayoshi Kohno -- let's say that an innovation that is really taking off, you kind of want to catch it when it's far enough along that you know it's going to be a thing, but early enough so that you can actually have some effect on it. Because once it kicks off and it's out there. So, this is one of those instances where I feel good that we caught it at the right moment, because I feel that as people are adopting this technology and hoping to refresh laws in light of digital change, we can recognize this. For example, where privacy and security legislation can pass, my sincere hope would be that they would incorporate adversarial machine learning as a component.

**Rene Peters:**   One more question from me, and then I'll give other folks the light. But you bring up a natural second question about the timing aspect of this. You have to catch it early enough before it really takes off. I was curious, being someone who works with this policy lab and policy group, there are so many individual problems. What is your general perspective either federally or internationally on where we are in 2021 on being able to catch these things, and where are we going with it.

**Prof. Ryan Calo:**   I have to say that I love that question. I think it's super important. I would say that the hockey stick metaphor, as useful as it may be to talk to researchers about what issues to take on, it also embeds a kind of world view that I don't know that I totally agree with. There is a sense that technology is moving really fast and the law can't keep up. Indeed, the most complicated statement of this is from the 1980s. It's from the work of David (unintelligible), and he calls this a dilemma, which is the idea that if you try to regulate technology too soon, you're not going to do a good job because you can't anticipate its forms or its consequences and how people are going to interact with it. What's going to work? What's going to not work? So, if you intervene too early with a precautionary approach, you're going to stifle innovation. You're going to make mistakes. However, if you wait too long, at that point it's already going to be impossible to address. So, the idea is if you don't regulate Uber, Uber is going to be so popular that we won't be able to. It's kind of been rebranded as what is called a pacing problem, which is a more simplistic approach, saying that technology is so fast and law is so slow. A couple things about that, in my experience: First of all, technology is just one kind of social path. There are many others: religion, for example. And there have been any number of times when norms change rapidly, and law had to keep up. Like within a ten-year period, we banned drinking alcohol using the Constitution. We amended the Constitution to ban the drinking of alcohol, and passed a bunch of acts to make it so. And within a decade had completely reversed ourselves and gotten rid of that amendment. Similarly, there have been times when the world has responded to technological change extraordinarily quickly. So, between the realization that we could travel into space, and the space treaty that went on to govern space exploration, that was a period of seven years. It was incredibly fast to have the space regime after the introduction of a prospect of space travel. We were told that driverless cars were right around the corner so how could government ever keep up. We've been told that for like ten years. And it's going to be another ten years before we have widespread driverless cars. And you know what? Twenty years is plenty of time to plan for driverless cars. So, I think there's an overstatement about how fast technology is. There's an understatement about how fast law can be when it chooses, especially in a federal system where there's a federal government but there's also a state government and a local government like the one we are talking about here. Simultaneously, there's an overstatement about how fast technology is, and an exceptionalism that is not warranted. Ultimately, my view is that it's up to us. Anytime you want to intervene and channel technology toward human flourishing and in the public interest, whether that's in the beginning or whether that's in the middle, or whether it's later, that's up to us. At the end of the day, technology is just a social fact. It's a contingent social fact that we get to decide how it works. And I think that part of the reason that we have had such a handoff approach to technology in the United States is our collective inability to see the way in which technology is not inevitable and is contingent. That's a view I've come to in researching technology for about fourteen years, and I'm glad you asked about it.

**Rene Peters:**   Thank you so much for your perspective. If anyone else on the call wants to come off of mute and ask Prof. Calo a question, feel free please.

**Nicole Espy:**  I have a quick question from a privacy perspective. What laws exist currently to protect individuals, since this is the Community Technology Advisory Board. What laws are already on the books? Or should be pursued or developed to protect individuals that it could fall out from any type of manipulation of AI that's being used by the City or the County or the federal government. And then also, since this is also the Seattle City Council of Seattle level, what can local governments do in order to either implement laws or policies to protect their residents and their infrastructure from manipulation?

**Prof. Ryan Calo:**   Thanks, Nicole. As you are aware, and others on this call are aware, the United States does not have a comprehensive omnibus approach to either privacy or security. Hence it becomes sector-specific and activity-specific. So, there would be laws that deal with healthcare providers, laws that deal with finance, laws that deal with kids, and this and that, but there's no specific omnibus privacy law the way there is in Europe. That said, at a minimum, the Federal Trade Commission has interpreted inadequate security as being unfair under Section 5 of the FTC Act. So, there is an expectation that you have adequate security. Also, state AG's have interpreted inadequate security as being basically a violation of the many FTC acts, of their own accepted trade practice acts. But, at the moment there is no specific law requiring you to protect consumers from your own system getting manipulated. Do you see what I mean? If you got hurt in your Tesla because someone tricked the Tesla by putting stickers on the ground, it would probably be treated as a products liability issue. Was your design safe enough? Was this particular eventuality foreseeable for purposes of proximate causation. So, it wouldn't even be treated as a privacy and security issue. There are breach of notification laws, so that if you do shed information, most states require you to notify either the AG or the consumer or both, including this state. But those things don't usually encompass ransomware. So, for example, if you're at a hospital and your medical records have been hidden behind a wall of encryption, and your provider has been threatened by the ransomware folks -- give us $10,000, $3 million in Bitcoin, or we will never give you back access to your records. Even though it could affect your healthcare quality, there is no obligation under the disclosure laws to tell you, because technically speaking, none of your unencrypted data made its way into the wrong hands. You know what I mean? So, there's a disconnect a little bit. What you could do? You could pass local legislation that fills in these gaps. So, for example, you could pass a law that says if you're Seattle, and notwithstanding whatever Washington law says, if in Seattle, and you're a hospital and you're a victim of ransomware, you need to tell all of your patients. You could pass a law like that, right? But, alternatively, one of the things I like to point out -- and I notice the theme of one or more of your meetings is when you procure things, you are making policy. There's a great paper about this by Deirdre Mulligan and Kenneth Bamberger called Procurement as Policy. But the basic idea is that when you buy stuff, your insistence that it be resilient against cyber attack, that it be equitable, that it not be biased, that it be this, that it be that, your insistence drives the market and, in a sense, sets policy. So, what I would say is that as you're thinking about working with software vendors, and you're thinking about purchasing hardware products, you insist upon the highest levels of security broadly defined. So, information resilience. Because that is the best way for you to -- if you make software for cities, you're going to need Seattle to want to buy your stuff. You know what I mean? And if Seattle comes to you and says, I like your stuff, but I'm really concerned about this aspect of it, guess what you're going to do. You're going to change it. In part, also because maybe Seattle will go to Miami and tell them that this is what best practice looks like. So, I would say if you don't have the political capital to pass these laws, then use your procurement power to make sure that you're insisting upon a level of design, and also -- you know, one of the things that we have recommended to the City around open municipal data had to do with making sure that you standardize and have a modular contract around what your software providers who process citizen and resident data about their practices. Because what we found when we looked at the different terms and conditions in the privacy policies of all the vendors to the City, they were all over the place. For example, this is an example from years ago, but when you had a provider for Seattle some of them didn't mention what would happen in the case where they lost or had compromised citizen and resident data. Some said we'll tell you in three days. Others said we'll tell you within a reasonable timeframe. Some contracts said we own the data. Some contracts said you own the data. Some contracts said the residents own their own data. Right? It was all over the place. And, so one of the things we said was standardize that. Once you start to do that and insist upon that level of data hygiene and that level of information resilience, well then, the market responds to you, hopefully, and we get a better eco-system overall.

**Harte Daniels:**   How can the City also protect itself from foreign actors? It's well known that China is working with artificial intelligence across the spectrum and gaining information, as good as Facebook, in the United States on their residents. And even one small example of that is their work with (unintelligible) and ancestries back home, etc. So, what can the City do to protect the residents against foreign actors that are almost as good or better than the United States?

**Prof. Ryan Calo:**   That's a great question. What I would say is that there are different threat models depending on (unintelligible). So, what we've seen is that while there is evidence of foreign interference in US elections, particularly two elections ago, the purveyors of misinformation today tend to be politically and economically motivated, and tend to be domestic. And so, I would say that the greatest threat of spreading Covid disinformation, for example, in Seattle (unintelligible). Conversely though, there is an ongoing and increasingly sophisticated and just relentless cybersecurity threat posed by state and semi-state actors, foreign in origin. They are trying to break into US institutions, both commercial and government. And their purpose is to steal intellectual property, to conduct espionage, political espionage, and so on. And so, that is basically just very sophisticated state-sponsored hackers from a handful of countries. Even right now, as we are talking, there have been multiple attempts on Microsoft, the University of Washington, as we are talking. Right? And so, one of the things that I worry about certainly is the fact that as one tool of many, artificial intelligence will be brought to bear. We need to guard against that. I think we have a dearth of expertise, especially in government. That's why I always have to talk to government bodies like yours, that have so many technically trained individuals who are working within our government. You are worth your weight in gold. One of the problems with our government getting access to technical acumen is that is sit so widely in demand and so hard to come by. So, we need to attract people to government. I mentioned earlier that my colleague, Tadayoshi, was a member of an Air Force task force devoted to cybersecurity. Yoshi is like a famous hacker. He is a person who teaches computer science and security at the University of Washington. But the Air Force created an apparatus to bring in American experts like Yoshi to help us become more resilient. But it is a constant (unintelligible). I will say very quickly that I don't for a moment believe that there's a real arms race between the United States and China, for example, about artificial intelligence, where whoever has greater artificial intelligence is somehow going to win some war, but I will say that it would be naive to think that the Chinese government and its affiliates are not constantly always trying to break into systems, because they really are. It would also be naive to think that artificial intelligence doesn't provide them with additional tools that they don't have now. But a lot of what's being done, even today, is pretty 101 stuff. When we're talking about social engineering where a person is sort of cultivated to click on something that they shouldn't. At the moment, it's not like a three-dimensional chess game. That's just simply not the case. And a lot of what's happening really is in many ways conventional hacking, this being done by extraordinarily sophisticated actors. That's my understanding. The thing that we found in both the cybersecurity and the misinformation space is that this stuff is so hard to stop individually. It's so hard to protect individuals against threats to them by foreign actors that you have to do it at the level of diplomacy. You have to make it economically and diplomatically painful for these organizations to engage in disinformation campaigns, and to engage cybersecurity threats. Which is why it is so disappointing -- and I'm just speaking for myself as a citizen, not as a representative of anything -- I was incredibly disappointed by the blase attitude that the Trump administration displayed towards Russian interference with the election, because it is precisely at that level. You have to make it painful for Putin and his subordinates to engage in the kind of behavior that we get at a diplomatic and an economic level. Because actually, stopping them in the moment, given all of the soft targets that they have across our enormous nation. I'm rambling a little bit. But you get the sense that it's above our pay scale. The foreign state adversaries with that kind of resources and sophistication, you really have to come at it at a diplomatic and economic level.

**Rene Peters:**   We have time for one more question. Dorene, I see you had your hand up. Let us know if you still have your question.

**Dorene Cornwell:**   I am happy to defer to someone else, because I was going to predictably ask something about transportation and under-represented populations and I want to hear someone else's question.

**Rene Peters:**   if anyone has one more question, please be respectful of Prof. Calo's time.

**Camille Malonzo:** I have a question. First of all, thank you so much for your talk. I have a question on the machine learning model. You talked about the ways in which some researchers testing could have been hacked or could have been subverted. Is there a literature or options, or toolkit or something that technologists can use to test their models to be more resilient against these kinds of attacks? And not just diplomatic law kind of way to mitigate the harms from adversarial hacking.

**Prof. Ryan Calo:**   I think of these questions as being a little inter-related. The point about bringing diplomatic channels and economic channels to bear on foreign adversaries has to do with interrupting their incentives to go after our intellectual property and our data, basically, and to interfere in our elections. You can reduce peoples' incentives, but you can also harden targets so that it becomes a greater investment of time and effort. Part of the research agenda of the people working on adversarial machine learning is how do you harden systems against attack. In essence, it's an iteration on the classical modality, which, by the way, the whole issue of that threat modeling, Seattle's own (unintelligible) was a pivotal in coming up with ideas about that. But the idea of threat modeling, how do you think creatively about who the malicious actors are, what their capabilities are, what their motivations are so you can make your system more resilient against attack? And that resilience is both a function of what is the attack surface of the system itself technically, but also who are the participants in the system who could be attacked socially. And now I think you have to layer in what are the AI machine learning models that might have vulnerabilities and how might they be compromised. And there's some technical work being done. For example, if a machine learning model is good at detecting a particular pattern, one pattern in the machine learning model could be brought to bear and attacked is a pattern of manipulation. You see what I mean? People are only doing this pattern if they're trying to exfiltrate data from model, or whatever it happens to be. That's a pattern you could recognize. So, people are working on that. But you'd have to have parallel systems, because no system can do everything. So, you've got one system that say, I'm going to do my thing, don't mind me; I'm just going to determine whether this is a wolf or a dog. I'm just going to figure out whether this is a stop sign or a speed sign. And then over here, you're like, okay, I'm going to look over your shoulder, and when I see something fishy, I'm going to tell a human being. You know what I mean? That sort of work is being done at the technical level. It will take a toolkit that involves both technical resilience, but also law policy and even diplomacy.

**Rene Peters:**   Awesome. Thank you so much for your time and expertise, such a wealth of knowledge. I think all of our minds are kind of saturated right now in the best way possible. Thank you, Nicole and Camille for bringing in this fantastic speaker. You really struck gold, and I think this was really great for the board. One housekeeping item for you, Prof. Calo. Cass Magnuski, who takes our minutes is asking that you go back and look at your chat or DM. She wants to confirm a couple of names with you. It was a fantastic talk.

**Prof. Ryan Calo:**   Absolutely. Thank you, everybody, and thanks for your important work. I'm really happy that you're doing what you're doing. And again, we're here at the University of Washington. Come to me or Lassana. Thank you very much.

**Rene Peters:**   Thank you. Before we move to committee updates, at the top of our meeting agenda, we introduced interim CTO Jim Loter, who introduced himself, gave us some of his experience, and some of his perspectives on the time he is going to be spending in the post for the time being, and maybe for the future. I wanted to give everyone on the board and the attendees a chance to ask him questions while we're in the question asking and answering mood. One of the questions that I have for you, Jim, is pretty simple. You know the work that the board does, and having had experience with the board in the past, how can we be most helpful to you as you aim to quickly ramp up into your work now?

**INTERIM CTO JIM LOTER Q&A**

**Jim Loter:**   That's a great question. A big chunk of what we do in IT is pretty operational in terms of providing services to our departments, but especially in the areas of data privacy, surveillance technology, and I love Ryan's concept of procurement as policy. I think we have a lot of levers to implement better policy, in terms of the decisions that we make, whether it's to serve our internal customers like City Light or the Department of Transportation, or in those technologies that have a direct public face. Over the last few years, we have incorporated to this, too, our procurement policies. The Surveillance ordinance is one of those. We are now required to evaluate certain technologies and have had to develop some specific guidelines around what counts as surveillance technology. It's not an all or nothing thing. Products don't come with a big red stamp branded on the side of them saying this is a piece of surveillance technology. We've had to develop some sophisticated ways to break technologies down into their components and say, yes, this might be a people counter that you might want to put on the borders of a park, but fundamentally, it's a camera, and that is a piece of surveillance technology. So, rather than just say we're not going to buy it, we have had to say, in order to mitigate the risk to public surveillance, your camera has to collect data and process the data in this specific way and not transmit the data over, not store the data. So, that gets baked into requests for bid and part of the procurement process. So, I think for you all to have an idea of how the City does business, how we have to do business in a lot of ways, and what practices we can influence on a day-today basis in Seattle IT, I think keeping that dialogue open and staying concerned about AI to then advise us to say when you are considering technologies that may have AI components, or are fundamentally built on AI, here are the policy considerations that we think you should take in your procurement practices. That would be, just off the top of my head, a really fantastic role for this group to play. You have the expertise in working in the field, and you Rene, specifically, with these types of technologies, and others as you were introducing yourselves. I thought, wow, you are working with a lot of stuff that we don't  really get to have our hands on a day-to-day basis, but that somewhere, sometime, some City department is going to ask us to buy, and I think keeping that dialogue open  and recognizing the expertise that the CTAB members have would be a great way that you all could help us out. I got really excited listening to Ryan, but also really scared. I was thinking to myself, wow, it's great that we actually have this group that's raising these issues, asking these questions. In the past, we've had great success with members of CTAB actually conducting some research, either on your own, or as maybe part of an academic program you're affiliated with, and presenting that to us at the City, and saying we think this is an emerging threat, or we think this a really interesting area for you all to look at in terms of providing public service. All of those ways are great.

**Rene Peters:**   That makes perfect sense. This year, we have already been engaged specifically in some of the things that you mentioned, whether it's Internet for All, or the Surveillance Ordinance technologies. We can share with you some of the commentary that we've submitted to City Council and other areas of the City, just giving our perspectives. Definitely, we will keep the dialogue open. Are there any questions from board members or members of the public? You'll have to come back next month. We'll have Councilmember Pedersen come to talk about Internet for All, specifically. But the floor is open for members or members of the public to ask questions.

**Mitchell Harper:**   My name is Mitchell Harper. I work in the industry locally, for a major financial firm. I am actually involved in some procurement decisions and writing policy around procurement, so I have my head in this space. I have a few thoughts on this. I missed the first part of the meeting. Who would I contact if I wanted to reach out for more information about ways to connect?

**Jim Loter:**   Connecting with the City? David Keyes is the primary liaison. I think that's still true. Is that true, David?

**David Keyes:**   Interim, yes.

**Jim Loter:**   I would say on this call, Vinh Tang and David Keyes are our great conduits to make connections with staff within Seattle IT. So, I would start with them.

**Nicole Espy:**   I'm going to drop in the chat the Privacy and Cybersecurity subcommittee that Jim mentioned that deals with the Surveillance Ordinance. [ctabprivacy@gmail.com](mailto:ctabprivacy@gmail.com)  And a lot of it has to do with the technologies that have been onboarded. We would appreciate your input, as well.

**Jim Loter:**   Nicole, thanks for identifying yourself. I kind of consider myself to be a little bit of a procurement nerd. Even if it's just to discuss how other sectors handle procurement, and what kinds of considerations you have. I would love to just chat about that, and on any particular issues.

**Rene Peters:**   Any other questions for Jim? All right. Looking forward to seeing you back at these meetings. We hope we can share some resources that will profile some of the conversations that are online as recently as last month, you know, collaborating back and forth on surveillance technologies. So, thank you so much. I'm looking forward to digging in and getting to work with you.

**Jim Loter:**   Likewise!

**Rene Peters:**   Next, we will move into the formal committee updates. Since Nicole has so graciously provided contact information for the Privacy and Cybersecurity Committee, Nicole and Camille, you can give your update.

**COMMITTEE UPDATES**

**PRIVACY AND CYBERSECURITY COMMITTEE**

**Nicole Espy:**   Our committee, the Privacy and Cybersecurity subcommittee, have a lot of things we want to learn more about. So, we have quite a few guests that we are looking to invite for future CTAB meetings. So, that's the meat of what we have mostly been working on. Trying to find more people to talk to about cybersecurity and infrastructure with the City, and more topics around that. Our usual work surrounds the Surveillance Ordinance and evaluating those technologies. We've already submitted our memo, as was mentioned earlier, and we await the timeline for the next round of surveillance technologies to review. I don't know, Camille, if there's anything else?

**Camille Malonzo:**  Yes. We were really grateful for folks from Security who joined us at our last meeting. So, that was really great to connect with them. We are grateful for the connections there, and to learn more about the ways they are working on security and infrastructure. So, that was great. I think, like all other subcommittees for CTAB, we meet the last Tuesday of every month at the same time that we have CTAB meetings. So, it's 6:00 to 7:00-ish, depending on how long our conversations get. Nicole put our email in the chat, so if you're interested, you can go there. Also, Rene has our subcommittee's web links at the CTAB web site. I think that's all we talked about last week.

**Rene Peters:**   Glad to hear it. Thanks for the update. Next, we'll do the Digital Equity and Inclusion. So, Harte, you're back; or Dorene or Coleman, let us know if you have any updates. I'll give you the floor.

**DIGITAL EQUITY AND INCLUSION COMMITTEE**

**Harte Daniels:**  Coleman.

**Coleman Entringer:**   So, no new updates from the Digital Equity Committee. At the last meeting, we were just doing our DL updates, and other updates from Digital Equity for the City. And then, again, the committee is on standby to get involved and provide input on a new TMF grant process. We are still waiting to get more information on that, but it should be coming soon.

**SMART CITIES COMMITTEE**

**Rene Peters:**   Perfect. Thank you so much. And finally, I don't see Tyler Woebkenberg, chair of Smart Cities, on the call. Femi, I know you were in touch with Tyler about goings on at the Smart Cities Committee, so if you have any update or information that you were able to get, let me know.

**Femi Adebayo:**  No, I was hoping to connect with him, but we haven't had the chance to connect. Hopefully, we will get a chance to connect sometime soon. I will try to find time with him in our busy schedule to see when we can.

**Rene Peters:**   Perfect. Thank you so much. So, that will complete the committee updates, and we will move on to public comment. The Technology Matching Fund was mentioned in the update for Digital Equity and Inclusion, so I wanted to invite Vicky Yuki to give a quick update on TMF.

**PUBLIC COMMENT**

**Vicky Yuki:**   Thank you, Rene. I appreciate that. You're always so complimentary. I love working with you. I just wanted to share that one of our Technology Matching Fund applicants that we have offered a grant to has declined it, because when it wasn't awarded the first time around, they had just pulled it. So that would be Lake Street Collective. So, that spot has been taken over by Computing for All. So, they will be providing -- They have workshops that they offer to a cohort of students that are in high school, and they basically partner with companies to be able to provide -- they learn HTML and different stuff around digital and ways to collect data. They provide that service. They learn how to do it and they provide that to the companies. So, it's really interesting. It's like on the job training. So, we're really excited for them to be able to get the award.

We are still waiting to be able to award those grants because the grants are federal grants, we need to make sure that our contracts correspond with that and we are able to meet our obligations federally. We need to ensure that the grantees that we fund this year with those funds are able to meet those obligations, as well. So, they're waiting for language support from the CBO, the City Budget Office. So, we still anticipate mid-August for getting those grants out the door.

**Rene Peters:**   Awesome. We don't want to get in trouble with President Biden, so dot the 'i's" and cross the "t's." I wanted to just put you on the spotlight, Vicky. Thanks for the update, first up, but also just a much broader thank you. For those who do not know, Vicky has recently rotated off as CTAB's liaison, and just has been super helpful to myself and Camille, and really the whole board. She is the engine behind TMF, and it's comforting knowing that you're not going far away, just across Lake Washington. But, just thank you so much for all of the expertise, all of the perspective. We look forward to continuing to work with you just in a little different capacity. You are very much appreciated.

**Vicky Yuki:**   Thank you! I look forward to participating.

**Rene Peters:**   All right. Thank you so much. Time for public comment. I will open the floor to any updates, any questions, or any announcements that any member of the board or any attendees have before we adjourn.

**PUBLIC COMMENT**

**Harte Daniels:**  I put two announcements in the chat. A third one was that I noticed that there was movement on the federal level towards the right to repair. And I don't know whether this has entered public comment or not. If it has, then the CTAB Digital Equity Committee would want to write a statement of support. For those that don't know, the right to repair for those who might have access to devices, meaning device recyclers cannot reuse those devices because the information on their hardware is proprietary. But digital equity groups around the country are seeking this so that there will be more devices available to low income people. I'm sorry that I did not have time to do the research. Thank you.

**Dorene Cornwell:** Do you know what is the timeline for the public comment. Is that something we could....

**Harte Daniels:**  I don't know when the periods of public comment open. I just know the commissioners, I think, from the FCC are promoting it, etc. But since I have been entangled with some of the deaths due to Covid, I have not been doing the research on this. So, I just wanted to put a flag out there. If there is, then yes, there might be something that the board might want to comment on, since it has been relevant to the team on Digital Equity for a long time to have this law change. Thank you. I'm sorry I can't give you more information.

**Dorene Cornwell:** Oh, no, that's fine. Let's just hold it for the committee at this point. I've been doing this weekly thing called Broadband Breakfast. It's just every Wednesday. It's an hour with different representatives from different batches of issues related to broadband, the climate, and financing. Some of it is really technical, and some of it is really legal. And some of it is really financial. It's just called Broadband Breakfast. You should be able to find it just by Googling Broadband Breakfast, because I'm not going to go dig up the link. But what I'm going to put in the chat, if I can find the link, there's a Broadband Community Summit, and part of it's live and part of it is virtual. And it's in Houston at the end of the month. It's the sort of thing where some of it looks really interesting. It's probably totally worth your time. The virtual parts are free. As if we don't have enough already to think about. It did cross my desk. And the user experience with Webex is continually a challenge. Where is the chat? <https://www.bbcmag.com/events/summit-2021/home>

**Rene Peters:**   There should be a huge chat bubble at the bottom right of the window.

**Dorene Cornwell:** I'm using the browser version. I just found it. The chat window is open and now I can't find where to type.

**Cass Magnuski:**  It's right at the bottom. Took me a long time to find it.

**Dorene Cornwell:** Well, one of the things is screen magnification, as I only see part of the screen. So, I had to bounce around. Sharing that experience was uncomfortable, but thank you for putting up with it.

**Rene Peters:**   Thank you so much for sharing that resource with us. Feel free, any members of the board or any attendees, to use that resource.

**Dorene Cornwell:** One more thing. For anybody who follows the weather and stuff, King County Health has a ton of resources about how to deal with heat, including a whole bunch of pieces of information where the content is translated into a whole bunch of languages. It's a whole spreadsheet. So, if anybody wants to make signage in a language, I'll put my email in the chat, because it should be available through King County Public Health, but I got it as an attachment in an email. [dorenefc@gmail.com](mailto:dorenefc@gmail.com)  I have no idea why it's not working. It was behaving a minute ago. This is technology and that's just how it is.

**Rene Peters:**   Thank you so much for the resources. Were there any other announcements or public comments?

**Cass Magnuski:**  Vicky Yuki, are you leaving us?

**Vicky Yuki:**  Yes. I am. My lasts official day with the City will be August 19. So, next Thursday. I have been with the City since 2007, and it's been a pleasure and an honor. I actually started my partnership and relationship with the City of Seattle through working at the Housing Authority, but also serving on CTAB. So, I was with CTAB before I was hired by David Keyes.

**Dorene Cornwell:** So, where are you going, Vicky?

**Vicky Yuki:**  I have just some opportunities that I'm going to take advantage of right now that I really can't share. I want to just say that it has been an honor. Thank you.

**Rene Peters:**   Thank you so much.

**David Keyes:** It has been incredibly fortunate to have Vicky working on the team throughout the City.

**Harte Daniels:**  There have been many things that the Digital Equity Committee that we could not have done without her.

**Vicky Yuki:**  I appreciate that. But, I'll be around still. We'll see first where I land, and then I'd still like to be involved in Equity and Inclusion work. So, thank you.

**Rene Peters:**   We are super happy for you, and are looking forward to seeing you around. Everybody, thank you so much for your time this month. This was a great meeting. We have some good meetings coming in September and October. Councilmember Alex Pedersen is coming to talk about Internet for All in September or October. We have County Councilmember Kohl-Welles to come and talk about facial recognition legislation that they're working on. So, it should be fantastic discussions and great perspectives from in and out of the City. We're looking forward to seeing you guys then. Enjoy the rest of your August. And we'll see you soon. This meeting is adjourned. Thank you.

**ADJOURNMENT**