**September 24, 2019 Meeting - Seattle Community Technology Advisory Board**

Topics covered included: Privacy and Data Protection Panel Discussion

**This meeting was held:** September 24, 2019; 6:00-7:30 p.m., Seattle Downtown Public Library, 1000 4th Avenue, Seattle, Washington 98104

Podcasts available at:  <http://www.seattle.gov/Documents/Departments/CTTAB/podcast/cttab.xml>

**Attending:**

**Board Members:** Steven Maheshwary, Mark DeLoura, Torgie Madison

**Public:** Sean McClellan, Camille Malonzo, Adam Owen, Shay, Jamie Tyfe, Adam Schuster, Cynthia Spiess, Alex, Heather Lowe, Soohyun Ji, Josh Moyer, Rita Cagliostro, Tiron Rowe, Phyllis Jacobson, Mike Katell, Sara Bromling

**Staff:** Tracye Cantrell, Ginger Armbruster, Kreg Hasegawa, Liz Gruchale-Gilbert, Kristen Hoffman, Carrie Fry, Seferiana Day, Cass Magnuski

**27 In Attendance**

**Kreg Hasegawa:**  Hello! Welcome, everyone, to a collaboration between CTAB and Emerging Technology 101. My name is Kreg Hasegawa. I'm a librarian here at Seattle Public Library, and I host  series called Emerging Technology 101. We've been having topics from Blockchain, Artificial Intelligence, and this seemed like a perfect fit to talk about data protection. The next section will be on October 21, which is a Monday, and it will be bout Smart Cities. There's a sign up sheet in the back to get emails for all of these events. There's also an evaluation form. The library loves to know how well we did. Be honest and we'll try to fix our mistakes. There are bathrooms outside. Women's, I believe, is over here, men's that way. Gender-neutral one is on the third floor. And we close at 7:50, so if we get into a really engrossing discussion after this, just keep that in the back of your mind. Tonight, we're hosting the City of Seattle's Community Technology Advisory Board, which has assembled a panel on Data Protection and Privacy. We are very happy to have this taped by the Seattle Channel. So when we get to the discussion part, please do use the microphone. The taping goes through the audio system. So, I'll just turn it over to Torgie Madison now.

**Torgie Madison:**  I'd like to start off with a brief introduction by Steven Maheshwary. He will tell you a little bit about CTAB, and we'll begin.

**Steven Maheshwary:**   Thank you, Torgie. And thanks to all of our panelists for taking time to speak with us and to speak with you all, and thanks for coming out and turning up. My name is Steven Maheshwary. I chair CTAB, which actually stands for the Community Technology Advisory Board. Our board was founded around 24 or 25 years ago by the Seattle City Council and the Seattle Mayor to advise the Mayor and City Council on all issues relating to information and technology. Just a quick background on what we do: We have three subcommittees that are focused on topics of Smart Cities, Digital Equity and Inclusion, and Privacy and Cyber Security. And today is an example of what we do to promote issues and talk about issues of privacy and cyber security. But we also work on policy reviews, and promoting in general topics of public interest, community interest, and policy interests related to technology. We have monthly meetings, usually every second Tuesday of the month, from 6:00 to 8:00 p.m., in the Settle Municipal Tower, which is nearby. Next monthly meeting is still TBD, as we may be doing another special event like this, but starting November/December, we're always at the second Tuesday. Please sign up, if you haven't already, and we'll get you in the loop with more information. And if you do speak up, it will be great to record you for our minutes, so please definitely do sign up. And if there are any questions, I'll be right here.Thanks.

**Torgie Madison:**  Thank you. I'd like to start off the panel discussion first by once again thanking everyone for taking the time to be here today. This topic is going to be Privacy and Cyber Security, and also the Surveillance Ordinance, and how that relates to the citizens of Seattle, and what that means going forward for the City. It's also a set in the backdrop of Portland drafting its own privacy resolutions and San Francisco recently passing a ban on facial recognition by use of the city. So, I'd like to introduce my panelists one by one, starting on my left, and I'll refer to my notes so I don't get anything wrong. To my left we have Ginger Armbruster. She is the Chief Privacy Officer for the City of Seattle, and was previously the City's Privacy Program Manager, in which she was leading the effort to create the privacy protections that are being placed in the City today.

Going down the row, we have Mike Katell, who is a Ph.D. candidate and lecturer at the University of Washington. He has expertise in information ethics and tech policy.

Then we have Sara Bromling, who is a project manager at Rubica, a company that provides enterprise level cyber security services directly to consumers.

And at the end, we have Camille Malonzo. She's a software engineer at Microsoft, and an engaged citizen who has been actively involved with CTAB and contributed to work on the Surveillance Ordinance.

So, please welcome all of the panelists. Ginger and I will have to share a microphone. To start off, we're going to begin with privacy policies, what they mean, and what the City has in place. I'd like to start with Camille, and ask, What does privacy protection mean to you, and what privacy concerns do you have as a resident in a major metropolitan area like Seattle?

**Camille Malonzo:**   So, first of all, thank you so much to SPL and CTAB for hosting this panel. It's really exciting. I'm so excited to hear from subject matter experts on privacy in Seattle. I think for some this is a community discussion, so we'll be talking up here on the panel, but you'll also have an opportunity at the end to hear what the community feels and thinks and has questions about what we talk about here on the dais. So, I think we'll have a mic over there as well as cards, for those who want to ask questions anonymously. Or take notes.

So, going back to the question, what does privacy protection mean to me in the context of Seattle and other major metropolitan areas. I think I first think about what kind of data institutions might have on me, individually, as well as communities, and what kind of controls to  manage access and maybe even delete that kind of data. What's kind of frustrating as a citizen, is sometimes you don't know what that may be across institutions. We can think about it as that kind of data in the private sector, consumer data, and the kind of controls the individual companies are implementing to have more access to that data. But I think increasingly when we read articles or just have increased public discourse about how technology and data impacts so many parts of our lives. We have a higher expectation for all institutions to share with us what that data may be. That kind of comes up in different areas, but I think specifically, when it comes to the City or metropolitan areas, or urban spaces, I think about specific areas like policing and how that impacts different communities in our area. I think about all of the articles that come up about licenses. I think in July there was an article about ICE is going through our licenses to find immigrants, and that was traumatizing for our immigrant communities, was really impactful. And then, I think the third thing is I think about the ways in which the Seattle community--and I think Ginger is going to speak to this--how we speak to those frustrations and concerns We have our privacy policy and all of the work that Ginger's team does. But how else can we have that accessible for all of the community members?

**Torgie Madison:**  Thank you. The next question follows that and is for Ginger. Seattle is one of the first Cities to adopt strong privacy policy. You can go to the http://seattle.gov web site, where you will be able to see the privacy information area where we have privacy principles, the privacy policy, and a privacy statement. Can you let us know what the differences are between those, and what they mean for us?

**Ginger Armbruster:**   I would be happy to. Can I first take a couple of minutes and describe how Seattle got to all of those. It's something of a story, and I don't know who has been here from the beginning. In 2015, the Chief Technology Officer of the City of Seattle, was tasked with doing something to build public trust about the data we collect. This came out of a few different technologies that became noticeable--that the privacy community became concerned about. One was  a camera that was put on the waterfront, a series of cameras for infrastructure protection. And some of those cameras were looking into peoples' apartments, inadvertently. It was not on purpose. It doesn't really matter. There was a wireless mesh network that was designed for first responders to be able to connect directly into, and be able to continue to communicate when they were out of the base. There was  period of time and space when people were having a hard time connecting. It did other things, as well. But people were concerned that they were identifying our phones as we walked down the streets. And the final one, which I think was probably the clincher, was the Seattle Police Department, in their enthusiasm, flew a drone in Council Chambers to demonstrate this wonderful new technology that could be used for a variety of purposes. All leading people to say, okay, we've been closing data for quite a long time, but technology is moving at a pace. We need to address the fact that we're collecting a lot of information. So the Mayor and the Council came to the CTA and said, "You need to do something about data and public trust, and how we manage this."

I was the person at the time for this. And we worked with an external advisory board, and an internal board to come up with what would a privacy program look like for a City? And we landed on the idea that we should start with a set of principles. We should start with what we stand for, and this should have public input; this should come from some experts in the field, private sector, academia. We had the ACLU participate. We had Seattle *Times,* who are very interested in the public records. That's how they do their work. I can't think of--oh we had private sector, I mentioned. We had federal prosecutors with experience on the federal side and drone programs. We had all these folks come together and we came up with a set of privacy principles. And there are six of them. They speak to acknowledging the importance of information, that we understand that this is valuable and important. We speak to being clear about notice and content, all the  way to security in data. There are six of these. I won't enumerate them right now. But those are the privacy principles, and that set the framework for what is important to the City. And from there we developed the privacy program. That meant that now we need a privacy statement. We always had an online statement, but now we needed to address all the ways we collect data, and what we're going to do with that information.

So we updated our privacy statement, which is the outward facing commitment to the folks in the City who interact with us electronically and other ways. We said this is what we're doing. We're giving you clear notice. Here's what we do and do not do. So that's available.

And then, finally, the privacy policy is a little bit different than what we're envisioning from an outward facing document. This is inward facing to the City to say we're going to do this. We're going to review the stuff we bring on board. We're going to follow these principles, every new project, every new acquisition, we're going to be following these privacy principles to make sure that we're living up to our commitments to the City.

There are four of us on my team now to make sure that happens. We have a review process so that we are part of the gating process, so that any new technology that's not standard is to get a review. Any new project goes through a variety of what we call stage feeds, which are places where we stop for a minute and say how are we doing on this. Are we spending the money in the way we should? Do we have privacy in place?

So that's what I oversee, in addition to surveillance, which we will pick up in just a minute.

But each of those components of the privacy program are important in delivering the final hopeful product, which is we're managing and serving information in the way we said we would. For us, privacy is about the commitments we make to the public. Personal information is really anything that can be linked or linkable to an identifiable individual. Aside from the idea that yes, we collect social security numbers and your location, and we collect whatever it is you need to do to permit your dog, all those things--anything that can be linked or linkable to an individual we take under the umbrella of the privacy program with the understanding, as we all should know, we have a public records act that makes it very difficult for us to actually protect information if it is requested by way of public records. All lot of our efforts around minimizing collection, being very clear to people about what could or could not happen to the information we collect. Hopefully, that answers some of that. Thank you for your patience.

**Torgie Madison:**  I actually had a follow-up question. As I understand it, you were involved with the Portland privacy principles. Could you elaborate on that?

**Ginger Armbruster:**   Yes. I came back to the City. I was a program manager building these principles, did all that work. I went off to private industries. i wanted to understand what it is that's going on in the consumer data world that is coming back to the City. A lot of people are going off, getting that experience, and coming back to us with all kinds of great ideas. I wanted to understand that better, so I went to Microsoft for a couple of years, came back and what I had found almost immediately in the two years that I had been gone is that many other Cities/States.Municipalities were having the same experience we had had. The public wants to know how data is being used. We have those expectations in the private sector. Europe is taking great strides in consumer data protection. All of these Cities and States suddenly wanted to start their own programs. And I started getting phone calls. A lot of phone calls. Portland was one of them. And I went down for a day, and we spent time together on their information folks, data folks, equity folks, people interested in data equity, and we worked on their set of principles. They came from a slightly different perspective. I think ours was a little more surveillance-oriented with concerns about surveillance technologies. Theirs came from data equity perspective. Every City has their different intersection. They all kind of end up in the same place, but that's what that was. I have also had consultations with San Jose. San Francisco wanted me to take a look at their facial recognition legislation, just to get a perspective from somebody who has been doing this for a while. Minneapolis, Washington, D.C., probably ten or fifteen different Cities are working on similar projects. Not that we have all of the answers. It's just that we've kind of plowed that road, so we can give them ideas about what has worked and what hasn't, and things to think about. And the thing I tell all of them is to start with principles. Start with what you can all agree on. We can all agree on some things that are pretty basic in terms of your rights around data. It gets more complicated when you get into the details about how you're going to run that.

It was a great experience with Portland. We continue to collaborate. And we have, through the Future of Privacy Forum, a monthly conversation, which I think is 30 or 40 people now on this call, all sharing information about what people are doing, what is working, what are you hearing, what is successful with your elected folks, what's working for public engagement. We're all trying to collaborate and come up with best practices in an area that's absolutely brand new. We just are forging new territory, and that's different from private sector.

**Torgie Madison:**  Thank you very much. So this sort of dovetails into one concern, which is that if you live in Seattle, you might have a very strong privacy policy or privacy principles that protect you as an individual, and your data. But if you go outside the City limits, the next City over might have a different view on privacy principles that are less strong, or just prioritizing digital equity versus surveillance mindset. So this next question is for Mike. It has to do with what efforts are being made at the State level, the State of Washington level, that are also addressing privacy concerns, and might provide some more consistent privacy protections across the State of Washington.

**Mike Katell:**  Yes, thanks, Torgie. There has been a lot of activity at the State level in Washington. Even at the State level, we have the challenge of even if we pass progressive legislation in the State of Washington, there are still the States of Idaho, Montana, Oregon, California, etc., in every direction. I just want to clarify that passing something at State level is certainly better than only having municipal privacy regulation. At the moment, for the most part in the U.S, that's what we've got. We haven't passed any federal privacy legislation in the U.S. of any substantive manner, or at least in any way that actually protects privacy since 1986, with the Electronic Communications Privacy Act, which at the time was a very forward looking piece of legislation, but it was almost immediately obsolete. So that's where we are on the federal level. And anybody who knows anything about the politics of State, local, and federal law understands, all solutions that work on a fundamental level that actually protect people in a sweeping way, they have to be larger than local rules and regulations. We see the same problem, for example, with homelessness. You provide services for the homeless in one City, but they're not provided in another City. Then people move around. And then you have charges of creating a safe haven for homeless folks. But it does point to the fact that, the reality is, if you're going to have policies affect large numbers of people, you need regional, national, or international solutions.

Probably in response to the progressive policies that had been passed within the City of Seattle, there have been efforts in the Washington State Legislature that had been very promising. In particular, there was a comprehensive privacy bill that was offered and failed in the legislature last session that in some ways mirrors some very promising legislation that was passed in California that goes into effect in January, the California Consumer Privacy Act, which offers a range of data protections for consumers in the State of Washington. There's a good chance that a version of that bill--we know that it's pretty likely that we're going to see one reintroduced, and there's a good possibility that we'll pass something. Certainly, there is a certain amount of momentum happening from other States. Just like the Surveillance Ordinance in Seattle has joined with surveillance ordinances in other municipalities create momentum in other municipalities to do similar things.

Another bill, particularly progressive, that was offered in the State Legislature that I believe is quite remarkable and unique in the country was House Bill 1654, which was a moratorium--the original bill offered a moratorium on facial recognition technology use by State actors. And this is really important. For those of you who aren't familiar with facial recognition, it's  technology for identifying people based on their facial features. There are speculative uses of facial recognition that could go much farther than trying to identify people, to actually trying to determine things about them, like detecting their state of mind, their mood. Most of that type of technology is facetious at the moment, and years away. The identification piece is very much in place. Facial recognition technology is particularly dangerous. It's very dangerous technology. It has two sources of danger. One is the danger of its inaccuracy. It is a woefully imperfect technology, and it is unlikely to ever become perfect. It is particularly bad at identifying women and people of color and young people. And it has been tested over and over again and shown that white people are much more likely to be positively identified than darker skinned people, women, and children. The problem with misidentification is you can easily imagine  a scenario where somebody is wrongly suspected of being, perhaps, violent. Imagine a scenario where a policeman is wearing a body-worn camera, the camera triggers and says this person is wanted for an assault on a police officer. Weapons are drawn, words are exchanged. The possibility of violence is quite immediate. But even if facial recognition technology were perfect, even if it worked perfectly all of the time, could identify anybody anywhere at any time, you have to ask yourself do you want to live in a society which--and it could be applied to any type of camera or footage--would you want to live in a City in which any camera on any street corner was able to identify you, the people you were with, was able to pick your face out of a political protest, or to identify you entering or exiting a mosque, a synagogue or a social club. In this way, facial recognition is incredibly powerful technology, and so placing restraints on it seems quite reasonable. That's one of the bills that I think is likely to also be reintroduced at the State level. And it would solve some of the problems that right now some of the jurisdictions carrying the weight of reasonable surveillance and data and privacy policies, which is where we're at now. And I think there is very little else going on in the country. Ginger probably knows more about the stuff that's happening in other States and other Cities. I know that Illinois has a biometric identification bill that has now landed Facebook in court over their violation of that, but there is very little legislation that is sweeping in. It's probably going to be a long time before we see anything happening at the federal level, so these efforts happening at the State level and certainly at the City level, are where we can place the most optimism in regulating these kinds of technologies.

**Ginger Armbruster:**   Great overview, Mike, of what's going on out there. I thought I might add just a couple of things. If you are concerned about what is happening in the City, the City does not in any way employ facial recognition. At one time, we had technology that was limited to trying to identify folks who had been booked into different jails. We had several different counties that were involved in using that as one way to identify somebody who didn't have a positive identification. We haven't used that technology in two or three years. Just thought I'd add that from the City perspective. It's not tied to any other City, but that's one thing.

The other thing that I did participate in a session about facial recognition: It was a forum back east, and we were speaking about the technology, and I think the thing that does us the least good are all of the shows and movies that all of the amazing things about facial recognition. It doesn't do that. It can't fill in shadows. It can't fill in half a face that's not there. But I think it's the future of that technology that we're all concerned about and how it can be used or misused. So, it's definitely front and center, I think, for a lot of concern. I just wanted to let you all know that's something we don't do at the City. Don't concern yourselves about that. Or be concerned, but that's not what we're doing. It is a technology that only works face on. So, I was at this forum where drivers' licenses was the best use, or social media. Your wonderful, smiling face on your social media pages are the best images for that reason.

**Mike Katell:**  It was actually really interesting that the City had the booking photo comparison stuff that was on the master list, right? But now it decided not to use that technology. But the City doesn't actually have a ban on facial recognition *per se,* but it would be subject to the Surveillance Ordinance presumably as a surveillance technology.

**Torgie Madison:**  Thank you very much. Does anyone else have any thoughts on facial recognition at the State level legislation? Okay.  So, we've talked a lot about privacy policy in the context of a municipality for making a safe space. So, I want to transition a little bit and talk about what the privacy policy does for you in the private sector. So this question is for Sara Bromling. Rubica has a strict privacy policy, and data sharing policy. How does Rubica's privacy policy differ when you're signing up for service, and what do you feel most consumers out there agree to without realizing they're agreeing to it?

**Sara Bromling:**  Thank you. Can you hear me? I think, generally, most privacy policies are pretty loose in how they protect user data, and probably even weaker when it comes to who and how they're sharing that data with, particularly when it comes to third party vendors or advertising partners. Usually at Rubica, we sell security to our clients. In essence, what that means is we're selling trust. In part of that--a lot of discussion around this, but we decided literally to put our money where our mouth is. In our terms of agreement, we explicitly lay out that we will never sell your data guarantee to our clients, even going so far as to say we will pay our clients up to three  times as much as we have received for that data. But regardless, we adhere to a a strict 'we will never sell our clients' data.'  As far as why you may or may not ever be agreeing to, the first thing that pops into my mind is advertising partnerships and what that looks like. And when you think of free services out there, that might be from the games that you play, to the email services that you subscribe to, to a mortgage calculator. Any free service truly isn't free. What's happening behind the scenes is that they're gathering and selling your data. That includes some of those free security products out there, some of the free VPN services. The concept behind VPN is that you're protecting your privacy by using this technology. At Rubica, we think that's completely unethical to then go around and sell what we're telling our customers that we're protecting. So, in essence, I'd say that as a company, we have a pretty strict stance. We believe that digital privacy should be a priority.

**Torgie Madison:**  Thank you. Following that, this is a question for anyone who has a thought on this who wants to chime in. We've been talking about the ways that outside organizations or companies or cities are promising protections through privacy policies and data sharing policies, but beyond trusting those policies what can an individual do to protect their data from being collected and shared online either from a private company or from the City.

**Sara Bromling:**  The first thing that pops into my mind is due diligence. Right now there's a real lack of legislation or regulation around data privacy. Doing your due diligence when you are downloading an app, for instance, just taking the extra time to discover what permissions are you truly granting that app, and just being really cognizant that data is a real commodity. It's yours and you have a right to know what that data has been used for.

**Ginger Armbruster:**   And it's a hackneyed phrase that's been thrown around for at least ten years, maybe not that long, but 'if it's a free thing, you're the product.' No mistake about  that. If you're downloading a free app to manage your finances, to collect information in your family's calendars, the weather apps...think of all of them. When you download them, they want to know where you are, what you're doing, and then they track you going to and from your browser, to or from web sites. My daughter just got a hand-me-down phone, and we went through all of the privacy settings, and we had a real conversation about free. She's 13 and taking it in. I think kids are susceptible to this because they don't think about those consequences. So, if you have children or young people in your life, be aware that they think they know everything, but you know a little more. And then be aware that our privacy is not guaranteed. It's a wild west out there for all the information that can be collected for marketing purposes. Part of our review, we deal with third parties, is going through that exercise. we don't monetize; do you monetize, when we deal with a third party. And it becomes a little sticky. We like 'free.' The City likes 'free.'  We like free because we don't have a lot of resources and we want to give you as much as we can. So, 'free' becomes problematic when we realize, yes, it's your data that's getting collected in the course of 'free' and how we use it. I would say right on about reading those tedious online privacy statements. And I think that's really an issue right now. What is the concept of informed consent? When you check that box, do you really understand what you're doing? Probably not. So the industries are trying to take this issue on seriously, and I think there will be legislation around what that means.

**Mike Katell:**  Yes, and so far, that means a couple of things, but the short answer, to answer your questions, is there is not a lot we can do unless you're willing to do a great deal of work. And even then, it's pretty hard to protect your privacy. And it's difficult for people to make that decision on a daily basis, because for most of us, an individual bit of information about ourselves doesn't feel like it costs anything. Giving up my location, using my phone in all the ways it tracks me doesn't feel like it's harming me in any particular way. And I might be more sensitive to it if, let's say I was involved in some political organizing that was extraordinarily unpopular, or could run afoul of particularly powerful people who are very paranoid in the White House right now. In that case, I would be much more motivated to do the work, but for an average person just leading their lives, it feels overwhelming. In fact, what I hear mainly from students, the young people you're talking about--and these are people who are just sort of becoming really aware, people who are 18 to 22, they're becoming much more sophisticated about these issues, but they're still coming out of sort of a denial phase of paying any attention. And the first response is resignation. And I don't think that young people are the only people who are resigned. I think a lot of us in this room can relate to this feeling of 'what can I do?' And I can tell you as a scholar who researches this stuff, there is more data being collected about you than you know, in more places and more times. And there are more ways of collecting data about you coming at any moment now. So, pretty soon, lots of airports are going to be employing facial recognition at check in to get on a plane. I just read a thing today about how baseball stadiums are going to start using cashier list checkout the way Amazon does, which means they're going to have to scan you. And there are already things that many of you are probably already aware of, in which when you go into stores, and particularly chain stores, when you have your WiFi on on your phone, you are being tracked, and your location in the store is being closely monitored so they can tell what kinds of things are particularly interesting to you, and so on. But, of course, the more you think about these things, the crazier you're likely to get, and so at some point, you have to make a deal with yourself and just decide what you can live with. But some of the basic things you can do is that you can just be very aware, as Ginger said. Reading about what's happening, thinking about what the app is doing. A colleague today at the University of Washington just told me about a teaching technique she's going to try with her students this quarter. She's going to try something called 'the walk through.' She going to have people look at various apps and just walk through them. First of all just reading the various policies, but going beyond that, looking at how the app works. What kinds of information is it collecting? What is the experience it's trying to provide? What is required in order to provide that experience? And what value does the app maker get out of providing that experience to you, especially if they're doing it for free? By doing this, the advice is just 'slow down' in our use of all these tools and conveniences, and to be more thoughtful, and dare I say, 'mindful' about how we use these and what kinds of burden we're willing to take on. Truly, the question is a little bit problematic in one way, because at the end of the day, the real injustice is that it's actually up to us to protect ourselves against something that really shouldn't be as chaotic and wild west as it is. The absence of any meaningful regulation, particularly at the federal level, is actually a scandal. Even the GDPR in Europe, a very progressive piece of legislation, has gigantic holes carved into it to enable these very successful information and data businesses to go as unhindered as possible into their work. As if this is the only way we could organize society, the only way we could organize our economies was by just opening the floodgates and leaving individuals and groups open to relentless surveillance.

**Ginger Armbruster:**   We could talk for hours. One of the things I think it's important to do is to decide what's important to you. And I think if I were to give you just a few things to think about. The kinds of data that's collected even by app or by proximity or by using your online computer. Your person, privacy of your own body which is your own, you're going to the restroom, nobody's taking pictures. Online credentials, privacy of that. Banking information, and location. Just those. And to think to yourself, if I had to choose one, two, three, four, which one would come up to the top? I might suggest to you, and you may not be aware of this, but location data, when it's collected, it's usually to four or six decimal points. Four decimal points get within 20 to 30 feet. Six decimal points is within six inches. So, the data that's collected about location is that you're at the corner of Second and Cherry, it's you are exactly here in the world. It's an xy coordinate. It's longitude and latitude, and it knows exactly where you are. So when you turn on your location services, that is what it's doing. And those pixels that may be on a web site, that's what it's collecting to that kind of level. So you may want to be really thoughtful about what is most important to you. Right now, location data is super hot. Everyone wants to know where you are, so they can feed you ads and know where you're going to be next. The make inferences about you. When you rent a scooter in a City, or rent one of those bike shares, that's one of the pieces of information that's collected. The City likes that information because we want to build that infrastructure that we need for those modalities. Marketing companies like that information because they want to know who you are, and they start building this idea of who you are. And the facial recognition thing that worries me a lot is I don't want governance using it, because I don't think they are using it quite yet, enforcement circling. What worries me is consumer data that';s collected. My daughter went to campfire camp, and one of the first emails I got was, "Hey! Send us a picture of your kid, and we'll just feed you the pictures we take during the week of just her." I'm thinking, "What?" And you know, I had to get on my soapbox and call people. "What do you think you're doing?" Because what it does is building up a profile of a small kid, who really doesn't have any choice in the matter. And we don't know what that company is going to do with that data down the road. So, they may have a purpose for it now, but now it's just collected. I didn't do it, by the way. I told everyone else not to do it.

So those are the things to be thoughtful about: What is most important to you, and being mindful especially for that. Location is something you should be super aware of, just people knowing where you are and where you go, because you do that probably on a regular basis. Those chariot routes probably are pretty established about where you go and what you're doing. So, I guess I would say that it's not only the free stuff, it's everything else that's collecting information, and that you be mindful. You do have some choices. Not enough, I'm with you. We need some kind of regulation around this stuff. Part of it is, we were having this conversation, our legislators don't know enough about this, and they don't hear from people like you. And if they do hear from you, maybe it's not concentrated enough for them to see that this is really important, so there's a very small cadre of people who are concerned about this issue and understand it well enough. And I think there are a lot of people who have given up. I have people in my own office who say, "Oh, Ginger, it's over." And it's not over. There are choices that you can make about this. It does feel overwhelming, but there are some choices. And our legislators need to hear about it, that this is an important issue.

**Torgie Madison:**  No names.

**Camille Malonzo:**   I have a question. I think what is frustrating sometimes is this idea of self-regulation. That consumer companies can just regulate themselves. So, I wonder what you both might have to say about that kind of narrative and how we can combat that. Because I guess there are some companies that try to self-regulate, that kind of market themselves as having all of these controls over XYZ. Are they doing enough? Probably not, but what can we do about it?

**Mike Katell:**  Self-regulation is a fiction. When you ask the wolves to self-regulate around the hen house, you will still lose hens. There's no question about it. That being said, that's my strongest position. The keyword is 'self.' It's about self-interest. For example, the online advertising industry has, for many years, limited their targeted advertising up to the very edge of what they think people can tolerate. A lot of folks are concerned and believe that the microphone on their phone is listening to them, like, "I was just talking about a trip to the Sierra Nevadas, and suddenly I saw an ad for hiking boots, or a vacation to Sierra Nevadas. We're still not sure. People debate this. For the most part, except for malicious actors, no mainstream technology company or mainstream advertising company would turn on your microphone to listen to what you were saying. They're tempted. They want to, right? They're definitely having meetings in which people are arm wrestling over that issue. But they're not doing it because they know that would unleash too much hostility. So self-regulation means doing the worst you can do that people either won't know about or won't complain too vociferously. That being said, having given you my soapbox screed on that, at the end of the day, industry does have to participate in the solution. Whether or not they do it under some sort of duress is another question. Regulation will only go as far as the moment the ink was dry. Then someone will come up with a new way to mess with you. And there is a lot of work happening in the design field to promote privacy protection at the level of design. There's a movement called Privacy By Design that was initiated by Ann Cavoukian, who was a former policy maker in Canada, and now I'm not quite sure what she does except promote this idea of Privacy By Design. It does require a certain amount of good faith, the extension of good faith to companies, but companies are adopting this idea of Privacy By Design as part of their brand identity to promote themselves as the good guys. For example, Apple, which is not exactly a positive actor in all domains of its operations, has tried to position itself as being privacy-centric. Microsoft, to a certain extent, has also tried to do this, for not other reason but to differentiate themselves from Facebook and Google, and other companies in which they are in competition. But it's a branding strategy that is promoting certain ideas. Also, it does help, as people become more aware, things like the Edward Snowden revelations, have really put the idea of privacy on the map. It's been several years now, but it was really just a glimmer before those revelations happened.

Industry is stepping up a little bit, and at the end of the day, a lot of the changes have to happen deep inside where the technologies are coming from in order for it to actually be real and legit. I don't think that will happen completely voluntarily. It requires a good deal of pressure from consumers and a good deal of pressure from regulators. If nothing else, it threatens a much harsher sanction if they don't follow through.

**Torgie Madison:**  Great question. At this point, I think we're going to transition into talking more directly about the Surveillance Ordinance. A brief history: This is an ordinance passed by City Council on September 1, 2017, and it requires all City departments to identify technologies that they're using today that meet the definition of surveillance, and also for the future, any technologies that are acquired or hope to be acquired to meet these definitions to be reviewed by public comment through a working group that is focused on civil liberties. And then that assessment--it's called the Surveillance Impact Report--is given to City Council, where they can make a decision about whether to continue or not to continue, or to modify the technology that's in use. This is, I believe, very close to being one of the nation's first overall surveillance technology reviews. And over the course of these two years since it was brought, 29 technologies have been  added to the master list of technologies that needed to be reviewed. And I believe we are between groups two and three right now. In the review process, they are being batched up into groups and released to the public for comment. That goes for a month. Comment is collected and then passed on to City Council.

So, I just want to talk a little bit about this Surveillance Ordinance. This is a general question for everyone again. The surveillance technology criteria says that technology whose primary purpose is to observe or analyze the movements, behavior or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals whose identity can be revealed by license plate data when combined with any other record. That's the base definition of surveillance. When a technology matches that definition, it then goes on to a second step where it needs to meet certain inclusion criteria. And that means that the technology will be inclusion criteria. If it meets exclusion criteria, that means it is exempt from review. So this is open to everyone. One of the inclusion criteria states, again, that the technology raises reasonable concerns about impacts to civil liberties, freedom of speech or association, racial equity or social justice. The question is what does 'reasonable' mean to you, and who ultimately gets to have a voice in defining what 'reasonable' is to the City?

**Ginger Armbruster:**   Can I start it? Yes, that is a problem. The checklist he's looking at causes all kinds of consternation. When this bill was made into law two years ago, that was our first concern. Because what I might consider reasonable because of what the technology does may sound different to you all. We looked through these technologies, hundreds of things that can be construed, anything that monitored or analyzed or tracked identifiable individuals in a manner that could, we  kind of ended there. We figured almost anybody. If something is monitoring or tracking or analyzing your behavior for identifiable individuals probably resonates that that is uncomfortable, or could be construed, depending on what your activity is. If you are doing a political rally, and it's something that may not be popular with established government, that may feel uncomfortable even if that wasn't the intent. I think this law tries to get at intent, but we took the very conservative view that we are just going to count anything that monitors, analyzes, or tracks identifiable individuals, especially around police or other kinds of enforcement. We landed on four different departments that have these technologies. I think, in retrospect, to be very, very honest, that some of these probably shouldn't be on the list. We had three technologies from Seattle City Light that were used for current diversion, investigation, binoculars, and some metering devices that check electricity. It was a little bit of a stretch to say that was surveillance. But they're used for surveillance, right, for folks that are diverting current and not using it? So, I think it's really hard to do the sniff test on what feels like an invasion of civil liberties. And so, for the most part, the City took a very wide interpretation of that. That's such a hard thing to do, to try to capture the intent of something, and I think everybody who has different perspectives would have different thresholds.

**Mike Katell:**  It's a very good question. The word, 'reasonable' is found in a lot of legislation. It kind of signals the fact that our whole system of laws in the United States is really based on the idea that law making is always unfinished. The reason why so many laws wind up in court is actually not a failure of law making. It's actually by design. Laws are meant to be debated in courts of law, meant to be parsed by judges. That's why when we have the 4th Amendment of the U.S. Constitution about search and seizure, it's very short. Fourth Amendment jurisprudence is millions of pages long, and that's actually where we derive a lot of our privacy protections, in all of those court cases. So, the word, 'reasonable' really is kind of a place holder in there, which means we're going to figure that out later. But what Ginger points out is true about how the City responded. The intent of the Surveillance Ordinance is hard to completely understand, except that a lot of it is really spelled out in the very beginning of the ordinance.  At the City level, and the State level, and also the federal level, most bills are written with a series of proclamations of sorts, at the beginning. Declarations. In City ordinances, for example, they contain a number of paragraphs that begin with the word, 'whereas.' They make basically pronouncements about what led to the creation of that particular ordinance. And one of the 'whereas' in particular in the Settle Surveillance Ordinance is actually very profound because it actually points particularly to the fact that cities, law enforcement in particular, have a long and unsavory history of using technology to surveil and control undesirable populations. For example, in the City of Seattle and the whole west coast of the United States, the Japanese internment is a good example. In the years leading up to the Japanese internment in camps during World War II was at least a decade, if not more, of the federal government using the technology of the day to sort, categorize, and control the Japanese population of the U.S. We see echoes of it today in interest in controlling the census, putting people in camps, and so on. So the fat that that language made it into the Seattle Surveillance Ordinance is actually rather profound. With some colleague, I read surveillance ordinances from around the country. Seattle and Oakland are the only ones to have included this kind of language in their ordinances, calling out this troubling history. I applaud the City for this concerted approach of over-including technologies on their master list, so that scholars or activists could look at the list and say, "Binoculars?", why are binoculars on there? It sends a signal that there are probably things that aren't on there except those things that were exempted by the ordinance. But the City is not trying to hide the stuff that it actually has and uses. So, in that way, that's very positive.

**Torgie Madison:**  Thank you for that. That actually answered the next question I was going to ask you. I'd like to move on and talk about the remaining inclusion criteria that only one of them needs to be met for surveillance technology to be flagged for review. This is a question for Sara. The remaining two inclusion criteria that haven't already been mentioned:  How can collecting personally identifiable information, and this could be information such as a name, date of birth, driver's license numbers, Social Security numbers, or certain combinations of disparate things that can be combined to uniquely identify this person. One of the inclusion criteria, in particular, reads that the technology has a  highlight that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with contractually agreed upon services. And during the Surveillance Ordinance review, in the two groups made public so far, we've learned there are quite a few public/private partnerships or contracts made with third party lenders. So the question is, what sort of data sharing agreement would you expect to see, or would like to see in that kind of working relationship, and just overall, how big of a market is there for data sharing, and who might want it, and why?

**Sara Bromling:**  A loaded question. I guess I'll start with the first part, third party vendors and what you might expect from that relationship, particularly, I think, to a private corporation. Me, personally, I would say that that data is not being monetized, that that data is not being sold. However, when we're talking about third party vendors and we're talking about data breaches, they represent a pretty high number of causes for the data breaches that we do see. I think about in 2018, I think it was Best Buy, Sears, KMart, Delta, all different companies all hit with a data breach because they shared a third party vendor that supported their customer support and chat services. And just as recently as June of this year, the U.S. Customs and Border Protection Agency suffered a cyber attack due to a third party contractor. I've seen a lot of numbers out there, but I've seen a range from 45 to 60 percent of all data breaches have resulted from a third party vendor breach. So that is something significant to consider when we're talking about relationships with the government with these third party vendor agreements.

The second part, which is data and who would be interested in that, that is an incredible market. I think I mentioned data is now a commodity. I think it was back in 2017, *The Economist* wrote an article talking about how oil is no longer the most valuable commodity. It's now data. Whether that's accurate or not, there are tons of arguments back and forth, but nevertheless, data is a commodity. And it's a valuable commodity, so I think it's relevant to a lot of industries.

**Mike Katell:**  Yes, I just want to mention that I think everybody is interested in this data. Governments collect some of the most sensitive data about people that there is. Birth, marriage, death, right? Any kind of contact with criminal justice, any kind of arrest, any kind of business, trouble, bankruptcy. But beyond that, cities, of course, are getting to a point where they're not just involved in these transactions of your basic municipal needs. Cities have control over a great deal of lifestyle data just through the new forms of technology that they're employing. For example, smart electric meters, which have been recently adopted in the City of Seattle. All over the world, where smart meters have been employed, there have been a number of debates about the privacy implications of what smart meters can reveal about peoples' lives. Rather than a meter that sits outside your house and gets read by a meter reading once every month or two, they just do some math. A smart reader is capable of reading your electricity usage down to every minute, or even more frequently.

The kind of information that could reveal--and I should mention that the City of Seattle uses smart meters, and I don't we've settled on knowing what the reading interval was--but Seattle City Light has agreed not to sell the data to any third party vendors. But that is by no means guaranteed in other places where smart meters are employed. There is a great deal of interest because of what smart meters can reveal. They reveal, at the very least, what time people wake up and go to sleep. But smart meters can reveal more than that. They can reveal what kind of appliances are used in the home. It turns out that different appliances have energy use signatures that can be revealed through smart meter data. Mixed with Artificial Intelligence you can reveal a great deal. Not just one example, but cities are involved in all manner of collecting all types of data, new forms every day. On the one hand, we want cities to be efficient and effective, and of course, the ability to use and collect data is one of the ways in which government does its job. On the other hand, this data is very sensitive, and as Sara pointed out, it's very vulnerable. Not only are third party vendors open to security vulnerabilities, think about what you know about City government. Some parts of government are very well resourced and have incredibly sophisticated technologies working for them, and other parts of government do not. Other parts of government are not well-resourced, they're using outdated technology, their security is only as good as the last that they had from the IT department, and so on. I can't throw stones at Seattle, but this is true of government everywhere. Government only has the resources that the people give them, and they only have a finite number of them. So their ability to protect the data that they're collecting runs up against the same sort of barriers as happens in the private sector. But in the private sector, where there is bottom line profit incentive, in many cases, security is likely to be a little stronger.

**Ginger Armbruster:**   I think that data sharing also speaks to other government agencies, including the federal government, and so our interpretation is not only the private/public sector issue, but also where else could this data be used secondarily without consent, without understanding. We are very concerned about ICE action, for example, and coming after Seattle City Light invoices, and the recent story we heard on King County. I just met with the individual who is taking on the privacy role there. We put the law in place that says we're not going to share jail information that got shared with ICE many, many times. And then we had a driver's license State of Washington issue. So, I think the data sharing also speaks to being careful about the data we collect, and where it's used for the purpose for which it was intended. It's interesting, because I think the smart city idea, and that's coming up next, the next conversation.  Smart city technology can be wonderful, but it's collecting even more information than we currently are doing. So, the concern about what exactly that means, and what that means for the data the City collects--I want to remind everybody, too, about the Public Records Act. and it's wonderful to have a sunshine law that means you can know what the government is doing, most of the data that's requested is the public's data. So, every time we collect, we have to be mindful that somebody could ask for it. Please don't. But you can ask for quite a bit. And, as we look at smart city technology, that makes us super concerned, because we could write contracts all over the place about don't monetize, don't use it, but anyone else could say just give it to me. Give me all of the location data you have collected for all of those scooter users in L.A.  Give me all that data you're collecting for the bike share. We wouldn't be able to stop them. We have some contracts in place, and we're trying to be smarter about it, but that's what public data request means. It means that the private sector can get hold of this stuff without asking, which is what they're doing. They're asking for it, but they're not paying for it. I think about this late at night. I think about things like, well, if we're going to monetize it, why don't we do it for the good of the public. Right? If it's going to be made available anyway, let's think about being mindful about doing this in a way that we can finance some things. I don't know if that's the right answer, but it's what I start to think about, because you can't put brakes on some of this, unless we go back to the legislature and say, we know what the sunshine law was intending, here is what it has turned into now that all of this data is collected. Is that really your intent? Do you really want to make it so that everybody who is having a bad day with the police department, suddenly all of that is made available. I don't think that was really the intention, exactly.

**Mike Katell:**  And it was probably never the intention for it to become an industry. Those people collect the information and profit handsomely from it.

**Ginger Armbruster:**   I think the idea was that if the government is collecting information about you, you should be able to say, what information do you have, so I can know you're doing it the way you're doing it and you're not sending it out for some other purpose. But it has now evolved into something else, definitely an industry. We hear that some of those aggregators and some of those brokerage houses about how much information the get from public records and public records requests. Not meaning to depress anybody, but there you are.

**Mike Katell:**  Have you seen the new I-Phone?

**Camille Malonzo:**   I just want to come back to the Surveillance Ordinance. One thing that I find really confusing is the way in which the exclusion list works with the inclusion list, especially around two items on the exclusion list. What we can have a review on is body-worn cameras, and cameras installed in or on a police vehicle. That's excluded.

**Ginger Armbruster:**   Why is that, she says!

**Camille Malonzo:**   Yes, why, especially considering that the inclusion criteria is included if the technology disparately impacts disadvantaged groups. And the second one, the technology raises reasonable concerns about impacts to civil liberties, freedom of speech or association, racial equity and racial justice that we were talking about earlier. I'm reading this and it's very incongruous, and I don't understand.

**Ginger Armbruster:**   We could talk over beverages for hours about aspects of this law that seem at odds. I wasn't involved in writing this one, so I can't say that I was there. But I do understand. Imagine a room like this with probably about this many people, all having an opinion and trying to make sure their interests are heard and making sure we move forward on this, and real voices having issues. One of the things that came out of this is there are some technologies that are being governed in different ways. So, body-worn cameras have a whole different set of policy and I don't know if they're under ordinance, but there are strict policies and also private consent decrees involved, and other judicial oversight, as well as vehicle cameras for police. Those have an additional set of oversight involved with them. My concern from the beginning with body-worn is what we all were looking for I think was the bird's eye view of what's happening between two individuals. When we have a question about whether excessive force, etc., was used, it's actually facing this way. You may get some of what is happening back here, but for the most part, it's an outward facing camera. You're picking up all the additional information. However, those two technologies were exempted because there are other very stringent rules and regulations about how they're used and the oversight involved is even more than the Surveillance Ordinance. They were evaluated and are in place, separate from and even more stringently monitored than these. And additional exemptions are things like security cameras that are stationary or cameras that are on critical infrastructure, like bridges or dams that need to be in place. That's kind of the reason that those are exempted, as I understand it. Now, interestingly, whenever we have public engagement, we have nice people like you come to talk to us, those are the technologies that everyone wants to talk about in relationship to surveillance. And we have to say those aren't really under consideration, but I can talk to you about some binoculars. There are different technologies that are not addressed separately or brought into the City.

**Camille Malonzo:**   Yes, I think one really powerful part of the Surveillance Ordinance is the public comment period. And that's kind of how I got involved. And just having that public interface is really powerful because public records. So I think not having that for those technologies seems it didn't really engender a lot of trust. So, I wonder if that has happened before, and I was just not aware of it, but yes.

**Ginger Armbruster:**   Body-worn was handled separately. The body-worn cameras were in place, for those who don't know, that was a mayoral directive under several ago mayors. And it was, we will bring these in. But what they did do is they did something like 30 to 40 public engagement meetings just about body-worn cameras and concerns about those, to the point where it could be a full-time job for several people on the police force, but they did a lot of outreach about that one. Cameras on vehicles, I don't think had the same outreach. I think, if you have an opportunity, we will have more public engagement about surveillance technologies coming with the new year. You can talk about anything. You can talk about any of these issues of concern. Usually, we're highlighting a couple of technologies that are under review, but it's a good conversation to have if you have concerns.

**Mike Katell:**  I definitely think you're right to point out that there's something a little disconcerting about that exemption. Ginger is correct, of course, that there was another process that took place that is regulating to a certain extent how body-worn cameras can operation. But, one missed opportunity that I can see by not including them on our Surveillance Ordinance. And I should point out that body-worn cameras are included in Surveillance Ordinances in many other jurisdictions, but just not ours. One of the key features of our Surveillance Ordinance which is very powerful is the annual surveillance usage review, in which every item that is approved for use in the City has to be reviewed every year, and evaluated not only for its effectiveness, but also to understand whether or not it has any new features that have been added, any new capabilities that might not have been subject to the original review, but also reviewed for its effects on civil rights and civil liberties. To continue asking the question that the 'whereas' statement that was concerned with issues of discrimination and oppression were trying to ask, so that we should be able to say in using body-worn cameras for a year, two years, five years, ten years. And this year, we really started to notice a particular problem that we are uncomfortable with as a society. We don't have that opportunity under the way that body-worn cameras are currently regulated, because they are not in this particular ordinance. I should also point out another notable exception to this ordinance, which is that surveillance data that comes from other agencies is not covered by this ordinance. So, surveillance conducted by, say, the State police, or by federal authorities can still be used by the City of Seattle. I'm sure Ginger will correct me if I'm mistaken about that. And there is also no particular prohibition on...well, I'll just leave it at that. But, it's not the only exemption and there's a lot to be learned from comparing this regulation with the other very strong Surveillance Ordinances in the country, which is one in Oakland to see where there are interesting differences.

**Ginger Armbruster:**   I think the reason data wasn't included is that you could construe just about anything the City collects as surveillance. If you consider how much data is collected voluntarily and maybe through enforcement, that happens in various areas, from traffic enforcement to police. And I think the ideas was let's start with technology specifically designed and implemented for surveillance. I can't say that this is my ideal legislation. It's been cumbersome. It's taken two years. We did, however, get two of these SIRs voted on--I don't know if you know this--yesterday in full Council. So, two of these laws have actually gone into place with enforceable policies. It took two years to get these through, with many amendments, changes, rewrites. Not everybody is happy, still. I think this is in evolving, ongoing thing, and I think as our new City Council comes into place, there will be fresh eyes on this, and an opportunity for the public to provide their feedback about what is working for them and what isn't. Please come. Show up. Have your opinion heard. I think it's good.

**Torgie Madison:**   All right. I just have one more question before opening it up to a question and answer session. If you filled out a card and have a question on that, maybe Seferiana Day can collect those and bring them up. Otherwise, if you have a question that you didn't write down on a card, I'll be bringing one of these mics to the stand and we can have a 15-minute Q&A. So, the final question is for Camille. You are a member of the community who has found a way to get engaged and actively participate in these kinds of conversations. I would like to know how you started that journey, and what advice you may have for other people, who like yourself, may be out in the audience looking for ways to get involved.

**Camille Malonzo:**   I want to iterate first what you were saying earlier about reading and getting informed and doing due diligence. That was really the first job. Really questioning, "If I use Instagram, where is this data going to go?" And then I just kind of ball parked into this whole concern that I have.  I was so frustrated about it, I Googled Seattle technology and I came upon CTAB. I am very privileged to be able to go to CTAB meetings. I have the time to go to CTAB meetings, which are once a month Tuesdays, from 6:00 to 8:00. I was particularly concerned about privacy and so I joined the privacy subcommittee, that also meets on Tuesdays, the third Tuesday of every month, also around that same time. I just showed up. As everyone knows, just showing up is the biggest first thing. I got involved in the Surveillance Ordinance and did research on the various Group 2 technologies, and I am really excited about Group 3, whenever that comes up. So, I'll probably get involved with that, as well. And I also tried to find other resources around the community, so I know that the University of Washington has a great technology policy lab, and I'm on their distribution list, just getting informed that way, and how academics can have these perspectives is really good. I know that they have events that welcome the public. I've been to a few. There's one in October. I think those are the main ways that I get involved and be part of elections. Voting is very important. Those are the main ways that I get engaged with privacy.

**Ginger Armbruster:**   I think that's great. And if you're interested at the federal level, Representative Del Bene and Senator Cantwell both have partisan legislation they've been working on for quite a while. That might be a way to connect in at the federal level and see what we can do there. I think there's also going to be State action when that session opens up in January. They'll be working on legislation at that level, too. And there might be ways to connect or at least be aware of what's going on at the State level.

**Torgie Madison:**  Are there any final thoughts or statements from our panelists?

**Ginger Armbruster:**   I read a great article recently that the information we give out on social media is more than--and this is a dated reference--than the KGB ever got out of people under duress. And I think it's important to recognize that Mark Zuckerberg does not care about your social interactions. He doesn't care that grandma gets all of the pictures. He doesn't care that you are reaching out to your high school friends. None of this matters. He is gathering incredible amounts of information without giving it a lot of thought. And we're giving up our social interactions to folks. That really isn't the business they're in. I would just really recommend that folks think about those things. That may be a very important connection for you, but be thoughtful about what you're sharing. Be thoughtful about engaging in some of those activities. They are thinking out there in Silicon Valley now of all the new ways to get information out of you. And I think it behooves us all to be thoughtful.

**Mike Katell:**  I think I want to dovetail on that that we spend a lot of time thinking about how State actors use technology, surveillance technology. What I'm concerned about is the NSA, and ICE and the way they're using technology. And there's no question that the government's use of technology is incredibly impactful and incredibly serious. But at the end of the day, based on the most optimistic reading of our Constitution, we live in a democratic society, in which, in theory we have a say about how that work continues, how that work goes. And so, as Ginger pointed out, getting involved and speaking up and writing to legislators actually does make a difference. It actually does matter. But the more serious issue confronting us now is that now we have a private sector that has more data collecting and gathering surveillance capabilities than any government in the world. And this is unique. This is a remarkable moment, in which a handful of large corporations have incredible insight into our daily lives and the minutia of our existences. Like in anything, as a consumer the buyer needs to beware. You need to try to arm yourselves with as much understanding as you can. And be really, really skeptical about the words that come out of the mouths of technology leaders, no matter how cool they seem. Elon Musk, Mark Zuckerberg, Jack from Twitter, anybody coming down the line with the next great thing, when they use words like 'community,' ask yourself the question, "Whose community are we talking about? Whose happiness?" When they use words like 'freedom,' whose freedom are they talking about? Whose prosperity are really really addressing?

**Sara Bromling:** I would say, just to add onto that,  as far as it pertains to the private sector, I do personally believe that the consumer has a lot of power there. If the consumer can start educating and becoming aware of the practices that are happening in the private sector, the consumer can start affecting that bottom line. And at the end of the day, that's the driver for change for these companies.

**Torgie Madison:**  Thank you so much to our four wonderful panelists. [applause] I'm going to open it up to Q&A. I'm not sure how the mic situation is going to shake out, because this one is going up there.

**QUESTION:**  I have two inter-related questions for Ginger. The first is that -- and this is just my understanding of it, but GDPR applies to not just government technologies, but actually most of it applies to private companies operating in our physical location. Would Seattle ever consider legislation that covers the operation of private entities in addition to government? And the next inter-related question is, say you download an app, look at the privacy details, you don;t like what you see, however you have to use the app for work or for school. Given the decline in anti-trust, actually in this country we don't have a lot of consumer choice, especially in the tech sector, so if you're unhappy with the way a company is handling your data, who can you contact? Would it be the State Attorney General? Is there someone else, or some other form of advocacy that you recommend that you think would be most effective?

**Ginger Armbruster:**   Let's take the first one first. It remains to be seen if Seattle has interest in private sector controls and private sector privacy. We've concentrated on government because that's what we can control right now. I can make commitments to you and do my darnedest to make them follow through, and we can be transparent. You can see if I'm doing that. I have a feeling that the more local you are, the harder it is to get large corporations to comply. On the other hand, large corporations are already complying with GDPR. It may be that we are getting more of the local companies, companies that know they have to operate under certain terms if we have local privacy legislation in place. I think it remains to be seen. We do have a Mayor who is very interested in considering privacy. She, herself, has been victimized by a variety of activities, more around malicious intent, but I think that she has stated her interest in this area of privacy. Now that the budget is behind her, and she has her feet under her now for the first year. We'll see if that becomes something that's of interest to her. I do think that the State is a little farther along on some of this, so that's something to watch.

I just want to make a comment about Judy Carrera that it is more focused on the consumer. Europe has this idea that you have the right to disappear on the consumer side but they have a lot of information on the government side. We're kind of the opposite. We're more concerned about what government does and have not regulated the consumer side. When you consider GDPR, it's something that corporations are very freaked out about here. But I do know the large companies that you have interaction with mostly have adopted GDPR as the standard around the world. They just can't live with two different systems.

In terms of if you're not happy with app controls, the best thing is don't use the app. If you don't have a choice to do that because for some other reason you are forced to use it, lock it down as much as you can. And if you do feel you're being victimized, or you feel you have a complaint, I think I mentioned Representative Del Bene, Senator Cantwell, and State Senator Carlyle, and I can't remember the other ones, but the two folks who have been involved with consumer law at the Washington State level, would love to hear from folks. It gives them the justification they need to continue to pursue privacy laws. There's not a lot of power you have, excepting, "I'm not gonna play."  Maybe you can find an alternative. And let the company know. If you have a company, or at school--I had to do social media at the University of Washington when I was getting my master's. I was very happy about that. I jumped off Facebook. They made me jump back on because I was in a program where we had to communicate with each other. All of my old contacts came back. They never deleted anything. I know they didn't. So, some of it is pretty nefarious. But if you see activity that you really think is victimizing, I do think that our State Attorney General, who is in support of laws that we are trying to do at the State level, would be interested.

**QUESTION:**  This is a good discussion. It was talked about earlier about how people are willing to give up their privacy, whether knowingly or unknowingly, because they feel this immediacy of conveniences, they get immediate value. I think it's clear that there are also consequences, but they're not as immediate, they're not immediately felt. I bet there are lots of studies either being done or have been done that look at real, measurable consequences in aggregate, like across populations or communities. But people act in their own interests, not i the interests of the often larger communities or populations. So, what are ways that people should start thinking about or will eventually feel more of those consequences of giving up privacy, in a more personal way?

**Mike Katell:**  I'm going to try top answer that question. That's a tough one. At the end of the day, unless I get arrested for what I posted on social media, it's going to be hard for me to really feel that. That being said, the line of research that's personally important to me is understanding how the same technologies that are being used for, say, targeted advertising, in which we know where you've been, we know what you  thought, we know what kind of movies you watch, we know all of these various details about you. We've accessed your public records; we know your family composition, and so on, so we can send you ads for sneakers or for eyeglasses or whatever. That same technology is being used increasingly for a whole range of product, for things like employment recruiting apps. For a lot of people applying for jobs, particularly large corporations, HR managers are being sold these products that are designed to winnow down the gigantic pile of resumes. And how do they do that? Well, they do a number of processes like using AI to read through resumes with keywords and so on. Once they find a handful of candidates, hundreds of systems exist, products exist, that go out and mine social media data, using the same data stores that target advertisers use to identify people and  profile them, to render verdicts on people. And they're being used by employers, they're being used by landlords, they're being used in court rooms for risk assessment there. Most likely the way that people are going to feel these things, as these products and services expand out and touch more areas of our lives. So, we don't really have much control over making people more aware of this except by talking to our friends and families. But it looks like the industry is pushing deeper and deeper into our lives and we're going to start feeling the effects of these things in a more immediate way.

**Sara Bromling:**  That just got me thinking. I think, Ginger, you were mentioning these one-off data points. It doesn't really matter so much if somebody knows where I am this day. Or I turn on my location. But if you think about data brokers, and I'll use Axiom as an example, they're claiming to have like 1,500 data points on about ten percent of the world's population. So that means data points from sexual orientation, the browsing history, the medical records, the political affiliations. There are 1,500 data points on ten percent of the world population on this one data broker. And that makes me think -- there's this great documentary on Netflix called The Great Hack, and it really talks about Cambridge Analytica and the in-patch of what those data sets really, truly mean, and what that data could influence. So, I think it goes back to--it's not really in your face, but if you take a pause and take a bird's eye view of what's happening, data is incredibly powerful.

**Ginger Armbruster:**   Right now, we have an example that's come out of China about their social scoring. They're using all of this information to do social scoring, containing or restricting peoples' ability to travel. If you have a low social score, you're not a trusted citizen, therefore, if you're going to travel, you're going to travel in lower class. This is abhorrent to us, right? But, I think the kind of data that's being collected could lead to something like that. And certainly, HR decisions and whether or not you're going to get a credit score that can result in...we had a contest at the City of Seattle that worried me because of the precedent it was going to set. It was a Department of Transportation initiative with the best of intentions. We wanted to limit the number of accidents people have. It was the safest driver contest. It was fabulous. It collected all of the information on your phone, this app that was going to look at it whether you were cornering too quickly, you were stopping too much. And somebody got $2,500 for making the best score. And all I could think was Pemco and Google were the sponsors of that app. Right? All you could think was that was a foray into probably some kind of insurance scoring that was going to decide, whether or not you were in an accident, how prone you might be. We're really good at the scare stories. Sorry. But I think those are things to be aware of, that every little bit of information that's collected out there could have a purpose. So that's why you want to be mindful. I'm not saying you shouldn't sign up for that contest. $2,500 is $2,500. But I believe you want to be aware when we do that. What's being advertised is this great thing, but there might be other reasons why companies want that information.

**Mike Katell:**  One more comment about that: I really urge you to support tech journalism. So, if you're not currently a paying subscriber to a publication like *The Guardian,* which has an excellent technology section, or the Washington *Post*, which has excellent technology coverage, or even any smaller publications, even some of the better blogs out there, a lot of great information that comes through people whose job it is to look for the smoking gun and to interpret it. I've read some--some of my education comes from outstanding tech journalism that I've read about these issues, so that I feel it more than I might have otherwise.

**Ginger Armbruster:**   One last comment: People tend to relate to their vulnerable relatives information being collected more than themselves. So, the one person I mentioned to you, who said, Oh, Ginger, it's over," I said, what about your kid? She went, "Oh." Sometimes that's the story that can get through to people. Would you want your grandma's information; would you want your elderly relative; would you want your younger relatives' information collected without them knowing, and used for purposes that may harm them in the future?

**Torgie Madison:**  All right, I think we have maybe five more minutes. We'll be running over a little bit, if that's okay with everyone. I think we can take these two questions.

**QUESTION:**  Hi, my name is Janice, and I'm not attending CTAB. I'm just traveling too much. What I wanted to say is, first of all, I had to laugh that this was promoted on Facebook. I'm involved with health systems improvement now. We went nationally and locally I'm also involved, so I actually suggested that we should have something on health tech in the future because a big issue that you just mentioned, Ginger, about the private sector. The big thing now in health is everything other than your clinician visit or your nurse visit. So, when you go to the grocery store, QFC or Safeway or whoever, and buy something, that's data. When you get on the bus, that's data. Almost anywhere you go, your phone is tracking what you do, where you work. In reality, somebody is capturing that, and they're aware of what we're doing and where we're at, and we're being judged somewhere on a a risk factor of where our health is, and how insurance companies see us. It's a huge field, and it's totally a wild west, and 'give me my damned data' is a big cry among us e-patients, but there's a huge other side to that. I'm just curious if anybody has any input there?

**Mike Katell:**  I have a thought about that, which corresponds with a question of research ethics in this field. Just yesterday, or the day before, I was reading about a new application. They were going to be using data about how people use their keyboards and collecting data from social media sites. I can't even remember what it was, but it had to do with providing information to clinicians. The whole idea was constructing this information gathering structure of peoples' every day technology uses to tell stories for clinicians to better understand the health of their patients. And it's being sold, of course, as something like, how can you deny health care professionals access to information that they could use to help their patients. But it raises a lot of red flags because we see a lot of this kind of research happening in which it seems like no one has stepped back to ask the question, what will the bad actor do with this. And whatever this technology was, the first I thought was, yes, the small number of clinicians who will use this to help a small number of patients will be completely outdone by the bad actors, who will use it to sell snake oil and products to folks. And the thing is, there's a great deal of sympathy or warm feelings about health data in the same way that there's a great deal of sympathy and warm feelings about when the police are able to reunite a child with their parents, using facial recognition technology, for example. These messengers are used to sell something. These technologies have so much goodness potential in them that we shouldn't question the dark side, but I would suggest that we actually always have to question and push very hard on the question of how can this be misused. And we should assume it will be misused.

**Ginger Armbruster:**   In the Ancestry site, be mindful of all your DNA. We don't even know everything it can tell us yet, but once that information is provided to those folks, it's out there.

**QUESTION:**  I just want to say something for 30 seconds, because everyone wants to leave. Everyone has some passions that are near and dear to them, whether it's environmental issues, or homelessness, or other things. And I've been involved with a key issue, both on the Seattle level and also at the Olympia level. And there are some things that I've learned, and my colleagues who have also been involved that seem to be kind of a framework against the public. That sounds very negative, but somebody who wants to see a legislator down in Olympia has to take a day off from work, because they're not working on a Saturday or Sunday. We are all working to try to live. So democracy is really great for those people who have jobs like yourselves, who can go to meetings and get paid when the public has to take their own private time, their transportation, their public parking, and then not be assured of talking, let's say, at the City Council meeting, which has happened. One other thing that seems to be pervasive is that the corporations, both in Olympia and in Seattle, and I'm sure in Yakima, have an ability to call up and have meetings with our government officials and create relationships with them. I'm thinking about the sign code and certain special interests that always seem to have access to the City and to the State, and help write legislation going back to that "I'm here to help you because you're really busy and we have the jargon." We just got some serious issues with Key Arena that the public wasn't even aware of. So, a lot of people want to be involved and participate, but they also have their daily lives, being a mother, being a husband, people are sick. So, I guess it's just how do you make an impact because a couple of Mayor's ago had one agenda, and then the next Mayor comes in and has another agenda. And as an environmentalist, I'm watching Washington, DC decimate everything that I've been working on for 20 years. So, I guess, how do we stay optimistic and hopeful, and participate in democracy and know that we can actually make a change as the public, versus the people who are driving the bus? Thank you.

**Camille Malonzo:**  I just want to say that you're totally right.  Even for the facial recognition, there was huge participation with Microsoft, and that was one concern for the ACLU in their public statement about the failure of the privacy bill. It's really hard for marginalized communities who have jobs and are the most impacted by these technologies. It's really hard to go to Olympia if you're in the environs of Seattle. It's so stacked against marginalized groups. I've been really inspired by our current slate of candidates for City Council, as well as King County Council and that's one way that being engaged with them has been really fruitful for me, because they know their stuff and I think they're really engaged. But I just wanted to validate that that is really so true that 5:00 or 6:00 on Tuesday is just not possible for a lot of folks. It's not very inclusive for a lot of communities. So I just wanted to validate that.

**Ginger Armbruster:**   I can understand that. My daughter is at home right now doing her homework. This is a hard topic. Public engagement in general is difficult. We throw parties and people don't show up, probably because the party is at the wrong time. But I agree with you that the opportunities for meaningful interchange with your elected officials is something that we've got to keep fighting for.  I do believe that they are out there. I do believe that this next slate of Councilmembers will provide their own opportunities for when you can interact. I know that our district folk have made themselves available on Saturdays. I don't know if everybody does that. It's something to continue to push for and let them know. I want to talk to you but I can't talk to you at 3:00 on a Thursday, because I'm at work. So what are some other opportunities? I do believe that the virtual world is giving us ways to communicate, at least asynchronously, but ....

**Sara Bromling:**   Corporations, though, seem to have a very easy pass.

**Ginger Armbruster:**   I'm with you. And that's why I think these organizations that can fund themselves, some of the organizations that have staff can help represent, but I hear you. And I think that's something that we've all got to continue to work on for ourselves. This is our community. These are our issues.

**QUESTION:**  Do we have time for just one more question?

**Torgie Madison:** Is it pretty brief? Would you mind ...

**QUESTION:**  I just wanted to point out that I listened to everything that you guys said. I was wondering if you guys had considered producing more icons that state data breach? And I say that in the sense of, there are a lot of people with a lot of different degrees, for example licenses for an agent, or am attorney. Looking at the other side of the coin, where if I am a licensed person to do a certain job, I shouldn't have access even on my private time to be able to breach into a person's life, even if I'm good at hacking. An icon that state, "You are data breaching," so a computer could pick that up. The other thing, too, on that is again an icon that let's you know that 60 companies have your data. Like the little flyer that comes up on your system, you look at it and go, I want to know who those 60 companies are, that allows you to track them and have a discussion with them. What are you doing with my data?

**Ginger Armbruster:**   I think all ideas are interesting. And I think right to know type laws that are seen coming out of Europe, cookie banners, etc., are letting people know. Some of that same notice in automated communication maybe will come this way through federal and State law.

**Mike Katell:**  I was trying to quickly search on my phone, but I don't I will be able to actually pull it up, but there's actually a browser extension, I think that goes with Firefox that helps you see all of the places that a web site is sharing information. There are a number of people who have done very interesting visualizations that show things like online journalism. Online journalism is actually a particularly bad actor when it comes to sharing information about visitors to their web sites. A number of people have written about how you can visualize and see all of the places, say a visit to Twitter, visits to the New York *Times,* results in information being produced across many different domains. But you're correct. People need to be equipped with more of this information, and we don't currently have enough of those tools, and we certainly don't have enough of those tools that are really easy for folks to just use and be fully legible and understandable. Privacy Badger is one, but there's also another one that's actually a visual. You click on tab and it shows you all of the companies that it knows of that are sharing information with the web site. There's another one with this beautiful visualization. It shows like this web of companies and how they're all connected.

**Torgie Madison:** All right. I want to thank all of the panelists and would also like to thank to co-chair of the Cyber Security Committee, Smriti Chandrashekar. She helped organize this event, but could not be here tonight. Give a shout out to the panelists.

**ADJOURNMENT**