>>SHOBITHA: Good morning, everyone.

Thanks for coming to our webinar today.

My name is Shobitha Parthasarathy and I am a professor in the Ford school of Public

policy and director of the science technology program here at the University of

Michigan. I am also the director of the technology assessment project. This is the

reason we are here today. Not discuss the publication of our recent report, cameras,

the classroom, facial recognition and technology in schools. Before we begin I want to

address the ongoing strike but University of Michigan graduated employees, that began

about 10 days ago. Use graduate students believe the pandemics reopening plans are

insufficient and dangerous. They want the University to cut off their relationship with the

police department. They want the funds of the University's division of Public Safety to

be reallocated. We are sympathetic to those concerns. We have fought long and

hard about whether to have the event today. We decided to go forward because the

issues we discussed in our report about law enforcement biased against people of

color, and racism and surveillance technologies. They are aligned with GEO's concerns.

Our overall aim today is to give you an assessment to the technology assessment

project. We call it topic. Methods of analyzing facial recognition and other echnologies,

to summarize our findings, and to talk about our conclusions and to knowledge E policy.

We will have time for questions in the end. Please leave questions and each time we

will get to them. Top as part of the University of message Michigan science and

technology program. As TPP is a unique policy center concerned with cutting edge

questions that arise at the intersection of technology, science, and policy. We have a

vibrant graduate certificate program, public and policy engagement activities, and

electro series. Our graduate certificate program is the jewel of our work. We teach

 students about how values, society, and politics shape technology and science.

Nylund students also learn about the signs I technology making environment. They also

learn how to engage in it. Our alumni now hold jobs across government of the

private sector, and non- governmental organization. Our program is anger because of

profoundly disciplinary approach we take, to teaching students about the relationships

between technology, science, technology and policy. Also because of the into

disciplinary about the students who in gauge. It engages students from the school of

information to the business school. 26 percent of our students come from engineering,

for example. In recent years, given the growing interest in the social ethic on equity

interest of technologies, our program has been growing. At present gift 73 students. As

TPP launched the project in the fall of 2019. This technologically driven world is

increasing at unease. As citizens we are aware more and more of how technology is

shaping our lives. We are starting to see how it has disproportionate impacts. It tends

to not just affect but reinforce any qualities. At the same time policymakers are confuse

how to manage technologies. They worry they cannot properly anticipate the

consequences to regulate it properly. It seems like technological development move so

quickly. How can there be adequate time for policy discussion and legislative activity?

On what basis should they be making decisions? Because of these things we wanted

 to do something. The idea of technology assessment as a general idea is not new.

They have used a variety of techniques to try do it.despite the social, environmental

problems. They use this analysis to inform their governments. We are try to do here is

something different. We are developing an analogical's case study method. Using

historical examples to inform our analysis of emerging technologies. I am a social

scientist myself, I use these kind of historical case study methods as my own

research, it is familiar to me. The basic idea is that the implications of emerging

technologies are much more predictable than we tend to think. We can learn from the

history of technology to anticipate the future. If we look at previous technologies we can

understand social patterns, and how technologies tend to be built, implemented and

governed. And the problems that arise. If we understand those things, we can do a

better job of anticipating those consequences. Before we get into the report, I want to

introduce our brilliant research team. They are all here today and you will hear from

each of them. Karen Forbes is a recent graduate of the Ford school public policy and

an associate in Chicago, background in tech. I want to emphasize, to analyze emerging

technologies. We also want to in Clement key disciplinary and writing skills. It is

important to note that Claire and Hannah did much of the case

development writing. As the top report is released at they have had the opportunity to

disseminate reports like these, and to engage with the media. other kinds of

commentary for public audiences. Of course, give presentations. Finally Molly

Kleinman is as TPP's program manager, she is also an expert in educational

technologies, therefore is a valuable part of the research team. We have a number of

people to hear from today. So, why facial recognition? And why schools? In so many

ways the idea of using a digitized image of your face to identify or verify your identity,

seems like the step of science fiction. It is increasingly used today from China to

Europe to the United States. It is used in a variety of settings, including most

notably and famously for surveillance and security purposes and law enforcement.

Also, for identity verification and our smart phones. Here in Detroit we have

project greenlight, businesses send footage to police. Digital images are checked

against law enforcement databases. The new use on the block, it's facial recognition

technology in schools. We have seen increasingly used across the United States.

It seems like a great solution. Perhaps most notably in 2018, a New York near

Niagara Falls, announced it would install a facial recognition system and its

schools. Cameras installed on school grounds would capture the faces of intruders.

Analyze if they match any person of interest in the area, have that much confirmed by a

human security person and that if there was a match, it would be sent to district

administrators who would decide what to do. The system was approved by the New

York State Department of Education last year, it finally became operational earlier

this year. Since and has been a subject of a lawsuit by the New York civil liberties

Union, and July the New York State legislator past a two-year moratorium on the use of

debates. At present, there are no national level laws. Exclusively based on recognition

around the world. Many countries are expanding their use of technology without any

regulation in place. Mexico City for example, invested $10 million and putting

thousands of facial recognition security cameras, to monitor the public across

the city. The state city system has been installed in 230 cities around the world,

from Africa to Europe. We did a comprehensive policy analysis of the national

international landscape. We wanted to look for policies that might be interpreted as

being related to facial recognition. We classified both proposed and past policies

into five categories. The first two are consent and notification policies which focus on

data collection, and data security policies that focus on what happens to the data, once

it has actually been collected. A number of policies in these two policies have been

passed around the world. Most notably the general data protection regulation in

Europe. Similar laws have been passed in India, Kenya, and also in the United

States, Illinois and California. European courts have found the GDP our club is facial

recognition. The third calorie is policies that Taylor use. We see this in the case of

project greenlight for example. The city of Detroit has limited the use of facial

recognition to investigate violent crimes, and also banned the real-time video

footage that was part of the original approach. Fourth, we see oversight reporting and

standard setting policies. These mandate different ways of controlling the

operations of facial recognition systems, including their accuracy. Most of these have

only been proposed. Finally, we see facial recognition use, bands, these have been

proposed at the national level in the United States. Where we see a lot more

policy activity in the United States is at the local and state level. Some states have

banned law enforcement use of facial recognition and body cameras. A number of

cities from Somerville Massachusetts, to most recently Portland, have enacted bands of

varying scope and strength. We have some policy activity but a lot of it is in progress.

None are explicitly at the national level. This raises some questions. We think about

 developing policy for facial recognition, what should be thinking about? How do we

know what we should be thinking about? This brings us to analogical case study

analysis. Analogical case comparison, we mean systematically analyzing the

development, implementation, and regulation of previous technologies, in order to

anticipate how a new one might emerge, and the challenges they will pose. When it

comes to facial recognition, we look at technologies that seem to similar in both their

form, and their function. We looked at how close circuit television and resources that

schools have used. What kind of social and equity problems they have had.

Once we developed ideas about the kinds of inflammations and complications that

might have, we looked at other sorts of technologies that had those implications and

tried to expand our understanding in that direction, as well. For example. Facial

recognition might create new kinds of markets and data. Looks at markets that have

been created biological data like human tissue, and genetic information. We try to

understand the implications of that. We did all of this interactively and we ended

up with 11 case studies, until we could clearly see five main conclusions from

analyzing these case studies. Claire do you want to take it from there?

>> Hello everyone I am Karen Forbes and I'm going to talk about the first three of our

five findings, why facial recognition has no place in schools. First of all, facial

recognition is racist and will bring into schools. Not only will it discriminate against

students of color, it will do it in a legitimate affair. Technology is so often assumed to be

objective and highly accurate. You may be thinking, isn't technology objective? Or

more objective than humans? The answer is absolutely not. Technology does not

exist in a vacuum. Facial recognition is developed by humans. Based on data sets

compiled by humans and used and regulated by humans. Human bias enters the

process every step of the way. Discriminatory racial biases are no exception.

We came to this conclusion that facial recognition is racist by studying the

analogical rate case. The policy that police officers can stop citizens on the street by a

standard of reasonable –. They discriminate against people of color because bias

enters their views. Many would argue that the staff is neutral because, if you are not

acting suspicious you should have nothing to worry about. However, that comes to

become untrue. It has been consistently proven to be raised disproportionately against

black and brown citizens. Take New York City for example. Throughout the use of this

policy people of color were stopped at higher rates than white residents.

Compared to the rates of crime they actually committed. Because it was susceptible

to racial biases of officers, it criminalized and discriminated against people of color at

high rates. Even though it was to be a objective policy. Facial recognition is

similarly susceptible to racial biases. It unfairly targets children of color. Finally, and

condition it has been proven time and time again to be inaccurate. Facial recognition

algorithms show higher alert rates for people of color. Black brown and indigenous

individuals, especially women, are misidentified. This will create barriers for students of

color. Because they are more likely to be misidentified by facial recognition, they are

more likely to be marked absent from class, locked out of buildings, or floods as an

intruder in their own school. Altogether it is inaccurate and ask and it will create barriers

against students of colors in school, we believe it should be banned. This brings us to

our second finding, facial recognition will bring state surveillance into the classroom.

We expect facial recognition will use this technology liberally. Conditioning students to

think it is normal to be constantly watched until have no right to privacy at school.

An environment that is so supposed to be safe and constructive. This is proven to have

negative effects on children. The analogical case study of the use of closed-circuit

television in schools, let us to this conclusion. CCTV is using most secondary schools

in the United Kingdom, facial recognition is virtually the same technology with much

more powerful capabilities, we felt this case was a perfect example of how putting facial

recognition in schools, will play out. This case reveals less that one administrators

are entrusted with powerful surveillance systems, it is hard to control how they use

them. We call this mission creep is the use of surveillance technology outside of the

original agreed-upon intent. Interviews with students at the schools though

these symptoms were limited for security purposes they were used for behavioral

monitoring and control. It was supposed to be used to find school intruders but was

rather use to punish students who violate a dress code, tardy, or anything else.

Students reported this use of CCTV, made them feel powerless, criminalized by

their school, and mistrusted. They reported they would change how the outdoor

dress at school, to avoid punishment. This heightened anxiety reduced feeling of safety

in school, it is likely to affect a child's educational quality. Because CCTV is just like

facial recognition, except for the fact that facial recognition not also surveilled, it can

identify students. Just like CCTV, administrators for facial recognition will be unable

to resist the temptation to use it outside of its agreed-upon purposes. We are positive

constant surveillance will make students feel anxious, stressed, and afraid.

This is where they should feel as safe as ever. This brings me to our third finding.

Facial recognition will create nonconformity for creating barriers for students who do not

fit into standards of acceptable appearance and behavior.

>> This is only the tip of the iceberg. It also has heightened when used on gender

nonconforming students disabilities, and children. Yes children. This is problematic

when this gets implemented into schools. We are confident that these will create

barriers for students who may already be a part of marginalized groups. Nationwide

biometric system is the largest biometric system in the world. They have fingerprints

and high facial scans over 1 billion citizens. It is required to access many public and

private services, including welfare, pensions, mobile phones, financial transactions, and

school and work environment. Like facial recognition, it is designed in such a way it

excludes certain citizens. Specifically, citizens who cannot submit biometric data.

Such as manual laborers or patients you may have damaged fingerprints or eyes.

This means these individuals who are already disadvantage, are now unable to access

 food rations, welfare, or pensions. Therefore, because these groups do not face her

and acceptability standard they face even more disadvantages in society, for no fault of

their own. We expect that facial recognition will replicate this in schools. When we

know from the CCTV example I discussed earlier that it is likely facial recognition will be

used in schools for behavior, speech, and dress code. We expect this will affect

students personal expression and get them in trouble, for not conforming to

administrators preferred appearance or behavioral standards. Altogether, because

facial recognition is likely to malfunction on students who are not white, or able-bodied,

we can expect facial recognition to affect marginalized students to be incorrectly

marked absent for class, prevented from checking out library books or paying for lunch.

We also expect children's will be directly or indirectly discourage for free public

expression. Overall facial recognition in school is for some students, and to exclude

or punish others. These will be characteristics outside of their control or their

personal expression. With I will turn it over to Hannah.

>> Thank you I am Hannah. There is so much detail, and great examples of everything

we are talking about today in the report. I encourage all of you to read it. I want to focus

on a few highlights for our cases, for the last two major themes we touched on. Let's

talk about how companies profit from data. A company cannot own your face, they can

own a representation of it. Like the one that is related by facial recognition algorithm.

A data point may not have may not be particularly valuable, companies can create value

by aggregating data, with a lot of data, or with different information that gives it context.

Individuals typically do not own any of the rights to their biometric data, despite this.

They often do not have a meeting will obey to give consent to collect and keep that

data. These new databases are vulnerable to subpoenas. We talk about the report

surveillance company called vigilant solutions. They set up a selling license plate

scanners to private companies. They connected all of the license plate data information

with all their customers. Knowing they all knew were all the scanners were placed and

how the geolocation information. They were able to recognize that they can use that to

build a new product, they gave real-time information about the location of cars

around the country. They packaged that product, they sold access to law enforcement.

The law enforcement product was so valuable they started to give away their original

license plate systems for free, to get even more data. They created a new data

market around license plate data that did not exist before. They were strongly

incentivized to expand it. We talked more about the implications of behavior like this in

the report, generally we do expect facial recognition companies operating in schools,

will also have a strong incentive to find secondary uses like this, for student data.

To get that valuable data they will try to expand their opportunities for collection, as

 much as possible by pushing to get into as many schools as they can. Paradoxically,

US ports have traditionally held that individuals do not own. The more versus the

Regents of University of California, 1990. In that case, Doctor Gold of UCLA used

 samples from his patients to develop a valuable research. He sold out and profited

off it without telling more about the research or potential profit. After he sold that he

would notify more of this use. Doctor Gold should've told him about the research

upfront, more tissue was considered discarded even when inside him, he could

not use it for anything on his own. He had no property right to it. Today a company or

researcher cannot use biometric data without consent. They do not owe anyone a

property state, or anything they develop using their data. Meaningful consent is

often limited, when it comes to complex technology systems, and especially in situations

like schools, where you cannot opt out of it. In the United States in particular, students

do not get a chance to engage with any of those questions because the family

educational rights and privacy act, allows schools to consent on behalf of their students.

Consent is not a topic for the student who may be surveilled. This push to expand

surveillance by companies, it will expand all of the reach of all the problems we already

mentioned. It also introduced some new issues of its own. Without strong data

productions this information is vulnerable to being stolen. It is impossible to replace

things like fingerprints and faces, once it is stolen it is out there. Second, data collected

 for one purpose will be used for other ways, at the same level of scrutiny, that is the

mission crew we talked about. Thinking back to vigilant technologies, many of those

private customers who use those initial license plate scanners, may not have signed up

to share the information. If they knew they were going to be generating data, that would

be sold and packaged to the police. Even if a company does not actually package I

data, for law enforcement use, one that has been collected they can subpoena that

information, and it is a lot cheaper and less politically difficult to subpoena them

build a similar database on their own. That is what happened last year with

ancestry.com, when police subpoenaed information from their DNA database to solve a

 crime, which would have been very difficult for them to put they database to gutter on

their own. You can easily imagine that police could subpoena facial recognition from

school to identify a student or track a child's whereabouts, if we are looking at the facial

recognition case. Our last theme is institutionalized in accuracy. In the report we

systematically unpack what accuracy really means, and what it doesn't mean.

Technology like facial recognition, we really talk about all of the ways that this idea is

complicated for a sociotechnical system. Accuracy could be in itself. I want to directly

tie what Claire said earlier about technology is being unusual from the human society

we are in. Thoughtfully and by sociotechnical system, directly to the questions about

accuracy, I want to show how these questions often get overlooked, leading to poorly

functioning technologies, becoming entrenched in daily operations. Components of

facial recognition also answer critiques about the technologies, by pointing out these

algorithms. They will get better and be improved by being used. Facial recognition

accuracy problem, deacons during the learning stage. That is early in development.

-- algorithm first to build a training data set, the system learns how to identify faces,

then you apply the algorithm to a testing side faces where the researcher knows the

identity, but the program does not. You see how often algorithm gets used. That is the

accuracy measurement that you are getting for most companies. The demographic mix

in the training site is going to determine how strong the algorithm is in various

demographics. Problems can vary. They are different from the real population

if you do not train with any women, you can still get your accuracy number two show

high levels of accuracy in your test. When you apply that system in the real world

where black women exist, you're going to have a problem. This is exactly what we

are seeing. The most common testing site is 77.5 percent male and 83.5 percent

whites. The main US agency, has not disclosed the Democratic makeup that

uses to test software it is difficult to test their accuracy. We do know that they built

in other database that was intended specifically to test how well facial recognition

performs, across racial groups and country of origin as a proxy for race. It did not

include any country is predominantly black, a high accuracy can also be hidden by

performance by one group. If that is outweighed by very high performance in

another group. You can begin to get the sense that it is very difficult to tell from one

or two numbers that I company might provide, or school district might have access to,

how accurate is this going to be across the population of your school? Another answer

to critiques like this, there should always be a human making final determinations.

However, when we looked into other forensic technologies, that use similar human

backstops like fingerprinting, predictive voicing or CCTV, it turns out across the board

when there is uncertainty in the process, forensic examiners tend to focus on evidence

that confirms their expectations. From CCTV studies we can get a sense of how well

humans might actually perform as safeguards for facial recognition, research shows that

trained observers identify individuals from footage, made correct identifications less

than 70 percent of the time. That number drops even lower when they are asked

to make cross racial identifications, to identify someone who is a different race of her

own. As a reminder., Even if a person incorrectly got identify they have already been

critiqued and sanctions that might have gone unnoticed. It also opens up a new

opportunity for human biases and punishment. In a facial recognition palette and South

 Wales, the police revealed that in the process of making only 450 arrest the

algorithms falsely identified over 2000 people. We get a sense of public this problem is

or could be. This is another way technology is fundamentally a part of human society.

Humans who are most susceptible to human identification are also those who are most

likely to face outside punishment. Another issue is the question of who who decides

what is accurate. Courts end up being the main arguer. In the United States trial

judges and the United States court system, the most standard to determine whether a

non-expert witness testimony, about forensic technology is scientifically valid for

the case. That is done on a case-by-case basis. They consider things like

potential air rates, the technologies of reputation and scientific communities.

They do not have a minimum criteria for determining any one of these categories.

As a result the accuracy of fingerprinting is ultimately determined by the legal system of

the equality of the lawyer and the experts involved in the case. Some states currently

accept fingerprinting and extra scientific witnesses while others do not. Suggesting this

is not fully reliable. It creates two separate standards of evidence. One for those with

the means to mount a strong legal defense and another for those without such means.

Law enforcement may have incentive to use technologies that they are consistently able

to get it in court with them. There is a lot more to talk about, what I'm getting eyes

accuracy is much more complicated. These translate human biases into the software,

and into the system of the software. Despite this, people tend to perceive, technology

as objective. It is inherently free from bias. Please have a long history of leveraging

this idea of objectivity in court, to argue that some arrest could not be biased,

because they were based on our current the myth prediction. This usually holds up in

court. I am going to pass it over to Molly to talk a little bit more about we anticipate

going forward.

>> Thank you. I am Molly Kleinman. Our recommendation is straightforward. Patient

and use of recognition technology in schools. In all of our research we are unable to

identify single use case where the potential benefits of facial recognition, would

outweigh the potential harms. This is true for the type of in person facial recognition

systems we are mostly considering in our research. It is also true for the kinds of

research that is expanding now in the online education schools, that are being used

during the pandemic. We have kids sitting in front of cameras all day. These

companies must not be allowed to collect biometric data for children, that have no

choice but to use their products. Furthermore, in this coronavirus situation we

are seeing other kinds of biometric surveillance expanding, such as thermal

tracking. Many of these systems have the same risk and dangers of facial recognition.

It would be best if countries banned them. In the absence of this, we are

recommending nationwide moratorium that would be long enough to give countries to

get advisory committees to investigate and recommend a regulatory system. When we

say an advisory committee. Talking about something that would be really

interdisciplinary. It includes experts in facial recognition technology and also in

privacy and security. Civil liberty laws, race, gender, education, and child psychology.

A moratorium should only and when the work of the committee is complete, and

the regulatory framework has be fully implemented. Separate from a moratorium

armband country should have security laws that address facial recognition and other

kinds of biometric data, if not already in place. The GDP art does not explicitly address

facial recognition, courts in several European countries have ruled that facial recognition

data is included under the GT PR personal data and is not permitted. Our report also

includes district level policymakers to help them provide effective oversight in the

moratorium. This is a situation we find ourselves in right now. As we discussed earlier

there is very little regulation happening at the national level or. We hope you look at the

report and ask questions. A list of Angelo's wills our goal of these listless to have them

ask questions even if it is only a single school building they are worried about. I'm going

to hand things over for questions.

>> Thanks Molly. Thanks for participating in the presentation, and talking about your

results. That is a pretty good place to start in terms of getting a general sense of

what the report talked about. As Hannah mentioned, we talk in much more detail

in the report about the recommendations. For each of these conclusions we looked at a

number of different cases for each. You will find those resources in the full report and

we have a shorter report. We have maps that I created a separate supplements.

As you folks are asking questions and the chat, I will say if you are interested in STPP

and its work, you can visit our website. You can see the URL here. You can follow us

on Twitter, and if you want to keep up to date on what we are doing and get our

newsletter, you can email us at STPP@UMICH.edu.

>> To think facial recognition should be banned across the world are just in schools?

>> Based on what we learned in our research, students are particularly vulnerable.

I cannot talk on if the drawbacks are going to outweigh the benefits, it is going to be just

as inaccurate, a lot of these things like feeling surveilled, and avoidance, a lot of the

cases we looked up we drew on cases that were not just in schools. We learned a lot

from people out in society, a lot of these learnings map directly onto other scenarios as

well.

>> I would say I agree with that. I would like to add, in some ways someone who

thinks about case comparison, using schools is just one case, it is a hard case, I agree

there is a lot of vulnerability among children, therefore I think use of technology

has to be at a very high threshold. I also think, we have offered a lot of

recommendations and they are pretty detailed. I think use cases that are more

complex, used in law enforcement, or even identity verification, we provided resources

that can be useful for those cases as well. This idea that humans are partly technology,

we have to address that in some way, the idea of data markets, these are things

we all have to think about in a really serious way. Regardless of the use of facial

recognition, my concern is that we are not thinking about those sorts of things enough.

Regardless of the use, you see that even most recently in the context of project

greenlight in Detroit, which is not the use in schools, a black man was misidentified

because his image was captured and it was linked to some older drivers license photo.

That kind of problem that we are identifying is something we see across facial

recognition uses.

>> The next question I have. Given private and public sector advocates of this

technology are likely to use the charge of inaccuracy and bias as leverage to highlight

how the tech industry is improving and training the human backstops is improving and

diversifying, the arguments against using the technology are being addressed, and will

soon be read the lesson relevant, so why banned this use outright?

>> I am going to take the director's privilege and say I think Hannah did a great job of

answering that question. The fundamental point we are trying to make is it

is impossible to reduce the inaccuracy in this technology. We cannot tech our way out

of this. There is no tech without humans and society, that introduces systematic,

structural bias, and individual bias. I am just using different words than what she said.

I do not think it is an argument. I hope our report provides some details to explain

why the argument is inadequate.

>> This is a question that is related to that one. Where do you think the attitude of

technology's objectivity comes from? Is there any sort of shift we are seeing in general

relation?

>> That is a great question. I could not tell you where that attitude comes from.

I think there is a belief in science tech and public policy field, we talk about the black

box of science and innovation that people assume what is done by scientists in a

lab is perfect. You assume if it is informed by science and research then it is not

likely to be inaccurate. I think it comes partly from black box policy. Chris is also STPP

argues for, we need to go ahead of this and regulate these things. Not just blindly trust

they are accurate. I do not know exactly where it comes from, but is it changing

generalization? We would all say yes. That is because we talk to STPP scholars all

day. I would like to think yes. Generations are getting more and more technology

advanced, for further use people use it every single day, and there is a better

understanding now that it is not perfect.

>> I do want to say that some groups have seen this as nonobjective.

It is not always news to every group. In general, a lot of people, scientists, and

tech, spent a lot of time in Silicon Valley. I still took my research now with people.

I very frequently find myself having to bring up the idea that tech is not

objective. I do not see there being a huge generational shift at this point, I do want to

point out that some groups that have often been harmed by things that are

called objective, have always known it is not objective. The idea that we are just

now learning this, is the idea that we are just not able to elevate this academically. This

is not just no, this is in science and technology studies as well. We are just now seeing

some of this be elevated in a more mainstream way. I think there's a lot of

power in the idea that your discipline is objective, the idea that we can build a new facial

recognition system or a new algorithm, the idea that it is objective gives us a lot of

power, to not only avoid some questions ut gives a lot of economic power to get

funding for projects like that. There is a lot of power that goes along with objectivity.

It does not mean it is intentional that people are trying to build up the objectivity, I think it

is a product of over time there is a lot of funding condensed around that.

>> I am calling this next question for myself. What do you make of tech that uses facial

recognition not in the name of security or law enforcement, more for specific teaching

and learning context that are often driven by faculty demand such as online exam

proctoring? I do not like those either. I think anytime you have a situation where you

are treating your students as probably trying to cheat, or probably criminals, you

are disrupting the relationship with your students, that is not a sound way to approach

education. I would argue that if you need this kind of policing technology, in order to

assess your students, you need to us assess your students differently. I realize that is

 easier said than done, there are incidents where it is difficult to come up with

different kinds of assessments that would work in an entirely remote situation.

We are dealing with a humongous expansion of remote education that people were not

prepared for. These tools can seem really convenient, like it is going to make life

easier and it's time or nothing in life is easy. I want to think about with who is making

the life easier, I want to center on the students experience when those technologies

are being used.

>> I will briefly say that facial recognition technology is ready being used in schools

across the United States pre-pandemic, and as you said yourself is only expanding now

at colleges and universities. The things that seem like seductive solutions, have

other types of problems.

>> This next question says I am from a place overseas where the government is

beginning to roll out smart sensors capable of being used for facial

recognitions, there has already been resistance locally, are there any simple to

understand resources that we could recommend to use to spread awareness of the

issues raised? Our report is a great place to start. [laughing] There are some questions

at the very and that are tailored for individuals acing these kinds of deployments.

It is focused on the questions they can ask unless specifically about advocacy.

I think it is a pretty short step from some of those questions.

>> I would at the end of the report, we have the questions that can articulate

some of the kinds of questions people might ask. I believe this is on the website but we

will add it, a one page summary of the five conclusions that might be a good one pager

to distribute in terms of resources. Somewhere in that report, all of the sections are

hyperlinks, we gathered a number of resources of add advocacy groups and others

during work in this area. I pushed everyone to make people think we are

thinking about these things internationally, there are some international resources

there that might be useful for those folks around the world.

>> A number of technocratic solutions are focused on diversifying data sets to better

identify black people, which unfortunately represents a form of predatory inclusion. Are

there strategies that advocates can use to highlight racist aspects of many of these

surveillance technologies.

>> I did see a lot of thought. Last year there was a big story about Google paying

a company to go into Atlanta and give homeless people five dollars to use

some kind of phone game, they were actually capturing their faces with a very

complicated consent, that they were not explaining. If the response to the

criticism of you being racist, is to go out and do something like that, it is hard to say

what is worse. That is a very bad outcome. I am not sure what I suggest as a solution.

If we can get this idea out there, not those clients of adding people to your database is

not sufficient to fix this problem, it would take a societal change to fix this. These

technologies are a part of society and totally indestructible from not. Next you can very

easily see that companies are not ready to not make a racist technology. I do not have

a specific solution, maybe a better understanding in general, it cannot stand on its own.

Plus I'm often accused of being a pessimist might come to technologies, I'm going to try

to be an optimist. When you see the report we offer policy recommendations. On the

one hand our instinct is to say there is something deeply wrong systematically and

socially, that cannot be fixed easily. We really need to think about stopping this.

We also understand what the real world looks like, and we want to address it. When you

think about a question like this, my initial instinct is to say we can use the analogical

case study approach that we are trying to pioneer here. I thinking through this I

thought to myself about two kinds of examples, one is infrastructure for

human subject research, it is certainly not perfect, it has a lot of problems. When you

think about the inclusion, dealing with exclusion by some sort of inclusion, or the

accretion of messed up incentives we have human subjects research system

has evolved, and has certain kind of institutional bias that we can take something that

has worked in society, and maybe innovate beyond that. Maybe that is one place to

start, if it is not a perfect solution. One of the ways that people have found not to

be a great solution, is the fact that it relies on individual consent and not community

consent. In recent years there have been ways to try to get community consent when it

comes to biomedical research. That is a another place but we might say okay, we

can think about how we will get community consent when it comes to issues

like trying to diversify data sets, of course, the diversification of data sets will not solve

this problem. If we are thinking about that we can use these analogical cases.

I also want to emphasize one of the things I am Trying to do, is to look across text

 sectors and look historically. That is key. Too often we are sidetracked by different

areas of technology, when we can learn across them, one of my hopes is not in

this effort we can start to look at examples that might look really different, but can

actually teach us some interesting things.

>> We have some questions We were not able to get to today. I will see if we can

follow up with you guys to answer those questions. Feel free to reach out to

us and get in touch. The contact information is all in the report.

>> Thank you all for coming. You know where to find us. Thanks everyone.