The Equality Arizona Podcast, Episode 5

SPEAKERS
Nicholas Bustamante, tanner menard, HLT Quan

tanner menard 00:17
Hello, everyone, this is tanner menard with Equality Arizona, and this is the Equality Arizona Podcast. Today we're going to be talking about surveillance, and it'll be a conversation between myself, our co-host, Dr. H.L.T. Quan, and Nick Bustamante. So with that, I'd like to just ask Dr. Quan, if you'd like to introduce our guest, and you can get our conversation started.

HLT Quan 00:50
Thank you, tanner. Again, this is hlt Quan and you are listening to Equality Arizona Podcast. Nicholas Bustamante holds a doctorate in jurisprudence, and also a doctoral student currently in justice study at Arizona State University. His work focuses on surveillance on the US Mexican border and privacy law. And I'm just so thrilled and excited that we have Nick with us to have this conversation tonight, and I know that one of the things that I really appreciate about our conversation is that you have a way of helping us understand the day to day impact of some of these heady issues that supposedly we are talking about. So I would appreciate it if you begin.

tanner menard 01:41
Thank you so much. Um, I've personally just had an interest in surveillance, you know, most of my adult life because I was 21 when September the 11th happened. And so it had a huge impact on my life. And I watched the rise of the surveillance states in the United States. I don't really know much about it. I've researched it a little bit of work a little bit from my poetic work, but I'm looking forward to talking about it. And I'm, I'm I would like to just start out by asking the both of you a general question about the origins of this surveillance state in the United States that like the initial laws, like the Patriot Act, and FISA, and if you could talk about the extent to which we are surveilled, and the extent to which we surveil one another.

HLT Quan 01:41
Okay, well, before before I ask Nick to comment on that, because that's why we have him here, I just want to say that when we think about surveillance, we think a Big Brother and the film 1984, which is a dystopian novel by George Orwell, and later made into the film in which mass surveillance is deployed to maintain a totalitarian, repressive regime, highlighting the ways in which information facts are manipulated. So terms such as New speak, number think, and double speak and Big Brother have been in many way repurpose to convey a mass surveillance and totalitarian tendency. But in our times, in these times, the time of big data and cryptocurrencies, not to mention a pandemic, which has global health implications, but also justification for surveillance, surveillance become one of the most important topic, I think, deserving of public scrutiny. So the FISA law, you know, we could certainly talk a little bit about the Patriot Act. And we can talk about the technologies that we have come to accept in our daily life. So let me just leave it at that and ask Nick to join us. Are you there?

Nicholas Bustamante 04:07
Yeah. Thank you both for for having me on here.I think that when we think about surveillance right now, especially in the the time that we're in, just as, tanner, right? had stated earlier, it's drawn back to 2001. And I think that the modern baseline for the big data surveillance that we have going on now, goes back to that moment, especially in the aftermath of 9/11, as the Snowden revelations revealed through the NSA's PRISM program, which allowed for domestic surveillance, but I think that going to someone's earlier point about not Big Brother, but how we are coming to surveil one another. I think another good point to look at is the use of algorithms in consumer prediction as another type of surveillance, and that going back going to Foucault's point on the panopticon is not, the point of the panopticon is also to shape behavior. And you have a rise right now, not right now. But for the past 10 years of consumer surveillance, that Shoshana Zuboff notes is a type of surveillance capitalism that's rooted in documenting every like that we have every purchase that we have to predict and ultimately shape future consumer behavior. And her larger point in surveillance capitalism is talking about the concern with that is not just about getting a new pair of shoes on sale, but what that can do to the democratic order, if these algorithms are used to say, influence the outcome of an election. And so I think it's important, it's important when we talk about surveillance, not just to talk about it in the sense of the Big Brother watching us that's that's a huge point, yes. But in the ways that we have allowed other companies to monetize our own personal data. And in that sense, it leads to how we surveil one another.

tanner menard 06:10
That's really an interesting point that you're making, Nick, about the way that we surveil one another and I'm interested, if you could just like, talk to a general audience of people that are using social media, who are maybe surveilling their friends, or surveilling their employees or surveilling their colleagues at the university. And I was just wondering if you could talk about about that a little bit? And then speak a little bit more about predictive algorithms?

Nicholas Bustamante 06:49
Yeah, well, I'll take your second point first, because predictive algorithms are a huge subject on to itself. But basically what it is, is, it's the mass generation and synthesis of hundreds of thousands of points of big data, and you use those you run through an algorithm to predict a certain model outcome that you're searching for. And we can get into later how that's used by law enforcement or how is using the criminal justice system. But basically, you know, you the way it works at its most basic level, is you see people liking stuff on Facebook, or on Twitter or on Instagram. And you're generated to more content that you are liking. And it's not necessary that you're going out and looking for this content. But the algorithm is set up to assume that based on your past 1000 likes 100,000 likes, whatever, based on your age, based on your ethnicity based on your zip code, you're likely going to like this. And so it's motivated, not necessarily on something that you actually may like, but on what layers of data are going are saying about you. It's a type of psychographic profile. And I think the former CEO of Google had said it best when he said something to the effect of, we know what you want before you want it. And I think that Dr. Quan will talk about that later. But going to how we surveil one another I think that one of the most, I guess, blatant ways that we surveil one another in the past year, have been the use of cell phones at protests. And initially, they were there to capture a historic moment for Black Lives Matter. And a historic moment for growing scrutiny over law enforcement, not just against black and brown people, but questioning the establishment as a whole. And you saw hundreds of thousands of people globally go out. And it was great in that people were able to share their experience across country across time and across space, but in doing that, people also open themselves up to a different kind of

surveillance. So what law enforcement did and agencies did across the country, is they used facial recognition software, to capture and analyze video what people were sharing. And they then used them, in some cases to go and arrest people at the protests. That's not necessarily even new. That has gone back. I think the earliest use of facial recognition software and predictive analytics to monitor a Black Lives Matter protest, I believe goes back to Freddie Gray, and the use of facial recognition software to not only arrest protesters, but also arrest some journalists.And what happened I think at the Freddie Gray Baltimore protests was they had just analyzed video online people sharing on Facebook or their social media accounts. And then they ran those faces or those names associated with those with the faces on that content through law enforcement databases, and then looked for people who had an outstanding traffic ticket or an outstanding criminal warrant, and they went to the protest and arrested people on that basis. So that's a double bind situation that we're in. And the ability to share content and to share data is so important to capture these movements where people are questioning systemic injustice, and rightfully so. But at the opposite end of that, is that the power to do that also comes with the power to aggregate that and deploy that against the people who are looking at the system critically.

HLT Quan 10:51
Thank you, Nick, for that. So I actually want you to kind of, I want to segue this into the work that you're doing. You're doing research looking at the civilians on the border, and one of the software company, surveillance technology company has been in the news a lot, and this is Palantir, whose co-founder and chairman of course, is Trump supporter Peter Thiel. Palantir works with the military, with Homeland Security with ICE and various intelligence agencies, and the Soros Fund Management recently, sold all of his shares, some of which have been held since 2012. Last year, the fund stated that the source from Fund Management does not approve of Palantir's business practices, and that it made investments when the negative social consequences of big data was less understood. And as you explained, not only are we better understand it, but it's also better exploited. And as you know, that activists particularly movement for Black Lives, activist, migrant justice, and of course, trans queer activists, have been vocally criticizing Palantir for working with law enforcement to analyze social media posts for everything from gang prosecution to coordinate operations and mass takedowns. But ICE also relies on Palantir software to execute workplace raids. And in addition to federal government, and its intelligence agency, they rely on Palantir software to mine data. Local law enforcement rely on Palantir technologies to organize mine and draw connections based on these algorithms that you are referencing, including using gang designations to lock up large number of Black and latinx people. And we know that trans women of color are frequently targets of police profiling and violence. And so we're going to take some of these pieces separately. The first one I want you to comment on, of course, is ICE and the technology, but also the kind of surveillance that are being done on the border. Can you talk about that?

Nicholas Bustamante 13:01
Yeah, I'd be happy to. I started researching Palantir through a group called Mijente, M-I-J-E-N-T-E, they are an immigrant advocacy group. And this group and other Latino immigrant advocates have I've seen the been the most vocal against the use of Palantir data analytics. But basically, what they do is they're a data analytic firm, and they create software platforms, and create a data ecosystem for ICE to capture details associated with the cases that they're assigned. So one of their program called the FALCON program, F-A-L-C-O-N, is used to help ICE organize their case loads, but also share data across platforms. And that sounds kind of benign. At first that it's, you know, it's just like any other online platform where people are sharing data. But where that data comes from is immigrants and the connections that they're drawing are to other immigrants so that the Palantir's Falcon program and their

Falcon tip line program and their case management platform system have been tied to document and data about children crossing the border, about family that they're staying with, about other connections they have in the United States under the rubric that that that system is used to vet human smuggling. So you have unaccompanied youth coming to the border or immigrant families coming in at the border and they're turning themselves in, you have the border patrol officers who will go and interview them. They'll collect personal information about them and they'll connect, collect information about people that they're supposedly coming to stay with. And the concern that I believe is that that the connections that they're drawing to other people are then used to aggregate and deploy workplace raids or ICE raids. Um, and that it's so it's not as as benign as the systems are just helping agencies keep track of data, it's how they're deployed against the people that they are surveilling, basically. But surveillance at the border. I mean, most of the surveillance technologies that I read, whether they be, I guess the best case example is our drones. They were initially developed for border patrol and later used abroad in the Middle East. But sort of the border is, in my opinion, the most ideal space to study surveillance, because the technologies that are deployed there go from not just tracking cell phone data, but to biometric data for people turning themselves in at the border, to capturing messages that are being sent across the border, to capturing people's stories who are turning themselves in at the border. And then those stories are later used and separated to tie pieces of data to other people in the United States. So it is a space fraught with surveillance.

HLT Quan 16:31
Can you talk a little bit about the specific, do you have examples, like somebody's story? So you could share with us?

Nicholas Bustamante 16:38
About the data being collected at the border?

HLT Quan 16:41
Yeah, yes.

Nicholas Bustamante 16:43
I think I mean, I initially got interested in the border because it occupies such a liminal space in fourth amendment analysis, you don't really have an expectation of privacy at the border. So searches can happen there just for basically any reason. And you don't need probable cause, you just need real suspicion that someone either committed a crime or crossed the border, which can mean basically anything. But what I looked into initially was the use of StingRay drones, or StingRays, and then drones at the border. There's a few different technologies, drones are like you see in the movies, they fly overhead, and they capture images from the ground up, and they're deployed to some other station where those people are just viewing those images and then directing the drone. StingRays are also known as IMSI catchers, or DRT boxes. And what that what these, what this technology does is that they mimic cell towers. And in spaces like the border where you have not that great cell service, what these devices do is they block out weaker signals by making themselves as the strongest mimic cell signal. And so if I'm driving from the border to Phoenix, then I send a message from the border and I'm near a StingRay device, that StingRay will capture my capture my message, and it will go to that, that StingRay. And then from there that StingRay can see the content of the message, they can see who I was messaging abroad. And then when that person's respond, they respond, they then have that message also. And

HLT Quan 18:30
that's frightening, by the way, that's frightening.

Nicholas Bustamante 18:33
It is frightening, completely constitutional. There's been suspicion that that suspicision's actually been proven that these StingRays have been used further and further away from the border. And I'll get into that in a second. But, um, well, my research found and I believe 2017 was that DHS, and CBP had the capability to use and they purchased StingRays with an airborne flight kit. And one of the drawbacks of the StingRay is that it has a limited space where it can block out a cell signal. So it's, it's only about 600 meters, but when you attach them to something that is higher up in the air that that that range grows, and when I found out was that DHS had the ability and and did purchase from the Harris Corporation, the maker of StingRays, were airborne flight kits associated with the StingRays, and there's documented documented use of StingRays being flown across the border I think between 2013 and 2017, they were done over 1800 times. But what the what the concern is that if you have a StingRay that is attached to a drone, and you're flying it across the border, one you're just picking up messages as you're dragging along. And through speaking to people who are forensic experts, and who the criminal defense community uses to vet StingRays is one like all of these systems, they're kind of shrouded in secrecy. There is nothing that documents how once these messages are captured, and I that's something else I didn't explain is that when, let's say, I'm talking to my dad from the border, and I send him a message, and he sends me a message back. They're not just capturing my message from the border. To be able to capture me, they have to capture the messages around me. And then they can focus on the unique identification number associated with my phone. So there is another privacy concern for third parties who are kind of in that dragnet in the beginning. And there's nothing that I found that shows that there's a documented procedure for deleting those messages for third parties caught in that initial dragnet. And that is the problem that I wrote about when, for one of for my dissertation, I'm currently writing my dissertation, rather, is that there is that concern when you're flying these systems across the border, is that they're just picking up messages. And there's nothing on there that shows what the procedure is to delete them, if they save them. And people that I've spoken to who work in the defense community basically have said that they there is no documented procedure for for the further deletion. And there's nothing saying that they're not using using those messages that were captured without probable cause or reason sufficient of a crime, there just happened to be in that space, there's nothing to say that new criminal cases aren't being built, or new cases for immigration are not being built based off of those other third party messages. So that is another layered concern. The other concern is that the Harris Corporation and other in the Harris is not the only corporation that makes these devices, there are a number, but these companies have non disclosure agreements. So if there's an ongoing criminal matter or criminal case that comes as a result of this, and you see that, you know, there wasn't a warrant issued for this, and there was justnwhat's called uh, it's not a warrant, it's called a, you ask for authorization under the pen register statute. And through that device, they were able to capture messages. And so what people in the defense community have learned is that well, if that generally means that they're, they think there's a stingray involved with this, they want to cross examine the expert who, who used that sitting right, say, you know, how did you get this information? Where did it actually come from? How did you come learn about my client? How did you kind of learn about this defendant, and there's a nondisclosure agreement that these companies had that basically say that, if that happens, you cannot go to court and disclose how these technologies work, where this information came from. And so it's a good tool for litigation. Because you can I imagine you can use it to get a better plea offer, based off of someone's unwillingness to testify. But the problem is that it implicates someone's constitutional rights to trial. And it also keeps the public kind of misinformed from

how these devices are actually used. And the the the scope of their use. And to tie it kind of back to what we were talking about earlier, is that stingrays and drones came back into you into the public scrutiny over the summer, when there was documented use at DHS was letting other agent other federal agencies use their drones to fly elver and monitor Black Lives Matter protesters. Something else that also came out of that was the use of stingrays. And protesters across the country had reports that their cell phones weren't working, let their apps weren't working. Or they would log on and off. And what I believe the New York Times wrote about this was that that was the likelihood was that police agencies in those areas, were using sting rays. They were just parking them in the back of trucks and just monitoring protesters as they were walking down the street. So you, I think from for me to understand surveillance. I initially got into it because I wasn't sure about the U.S. Mexico border. But in doing that it kind of led me down a rabbit hole to show that what's the surveillance that has developed and connected at the border is also intimately connected how to the surveillance strategies, not only used against immigrants within the country, but to other people of color, particularly Black Lives Matter, and an immigrant advocacy groups inside the United States. And so that's something that I'm still trying to think through and how to write about, but I think that it can be understood through surveillance capitalism, and that, like Shoshana Zuboff, spoke about that this new economic model that commodifies data is poses a danger to the democratic order. another facet of that, to me is the growing nexus between law enforcement agencies and data analytic firms who are similarly commodifying data, not necessarily to say you get a better deal on shoes, but to often mitigate against people's constitutional rights. And so that is particularly of concern.

tanner menard 26:07
I'm just curious if you could say for a moment, what does that mean for people that local police departments possess that kind of technology? And also, you know, there's automatic license plate readers and facial recognition technology in street cameras? What does that mean for us, like, just like being a citizen driving down the street?

Nicholas Bustamante 26:36
I think that, one, it speaks to how well, or how much law enforcement agencies are funded in this in this country, and that there have access to what is military or was once military grade technology. And now it's commonplace in the urban space. I think that it's particularly concerning from a constitutional perspective and civil rights perspective, for how these are being deployed, just because the secrecy that they're being deployed in, you don't always know how someone's data is being pulled in. Privacy law in this country is not great. Fortunately, Arizona has a explicit guarantee to privacy in our Constitution, however, how it's been interpreted is by our state Supreme Court has not always been as well fleshed out as, as people who are concerned with privacy would have would like it to see. I think that it's concerning when you see how it's being used against people to stifle civil rights. And I think that the ultimate, not the ultimate, but a externality that we need to take seriously, is how this shapes behavior, because if you are under the panopticon, constantly, you're you're going to change your attitudes are going to change. And you know, it may be it's great that it prevents criminal behavior, or maybe it's great that it stopped people from speeding, that, I mean, I don't want someone like my mom was driving a car to be hit by someone who's speeding that, that sounds awful. And that is awful. But in doing that, I think that there's a giving up of a certain type of liberty that is I don't think that the public has really thought through yet. What the implications for that are. And it's not just here, I think that um there. I think that what's what's the the algorithms that are being used in China, that there is more of a global consciousness going on to how our data is being used and what it says about us and the freedoms that we're giving up by letting ourselves be defined by disparate pieces of data that don't

necessarily tell a whole story. Again, these are run through algorithms. And the algorithm is to to achieve an end goal or achieve to achieve a definition within its Parameter Set, but they are set and they are set with a certain with certain types of biases. Um, but the another thing that I came across in my research was just how widespread that this surveillance network is, is that there are under the Trump administration, I believe in 2017, Elbit Systems, an Israeli based company, who has a US branch received an ICE contract to construct cell towers, in the border lands between US and Mexico on the Tohono O'odham reservation and that same company has generated and profited from the data systems that they've built along the Israel Palestinian border. And so these systems are being designed in a border context. And I think that people have to pay attention to what that means when systems are designed from a perspective to keep people out a particular group of people out and to monitor a group of people. And it takes on an added concern when it's not meant to only monitor those people, but then monetize the deployment of that data. So that is something that I think is worth consideration.

HLT Quan 30:44
Thanks so much, Nick. I do want to bring the Detroit's Project Green Light in at this point because I think it's a it's a good segue to talk about what does it mean to move these technologies that are at to use as port water patrolling and monitoring and and containment are determined to move into internally inside a community as a form of containment. So starting in January 2016, with eight camera systems, going live to city of Detroit deploy it Project Greenlight with the support of local businesses and other allies, essentially deploying video surveillance with real time face facial recognition by April 2020, is less than five years by the way, there were high definition camera in 700 locations across the city. This was coded as real time technology for public safety project in light in aiding and abetting the law enforcement stranglehold of city's residents, especially his brown and black residents. This is how the New York Times reported in 2019, quote 24 hours a day video from 1000s of cameras stationed around Detroit. at gas stations, restaurants, mini marts apartment buildings, churches, schools stream into the police department downtown headquarters. So the system works by connecting these cameras to so called real time crime center for monitoring. And this, of course, is a privatized security security system. Because participating businesses are paying into it to install the camera and agree to upload data to the system, which is then operated with the FBI, Homeland Security and other private security companies. And so big data algorithms are being used to to model potential crime hotspots and to identify suspects, like the Minority Report right away, anticipate crimes. And in 2017, a year after the Project Green Light began, Detroit contracted with DataWorks Plus for its FACE Plus facial recognition technology to assist in identifying suspects in real time. So this is this invasive surveillance that you're talking about, is being used to collect and compile data from the sources, multiple sources, right social media is another to process data. And then with the aid of algorithm to draw connections that purportedly demonstrate patterns and relationship of these communities have these people that are marked as different as target for surveillance and police patrol? Can you talk about that? Nick, can you explain to it a little bit more or? Because we know that the algorithm is not accurate, right, we know that the problem with artificial intelligence is misrecognition. Right? There's been a number of studies that have found that facial rec technologies have a tendency to reinforce pre existing biases are particularly racial and gender biases. The famous study by the ACLU in 2018, found 28 member of the US Congress, United States Congress mistakenly identified by Amazon recognition software as some as people who have been matched up those people who have been arrested for for a crime. So what does that mean? What are the implications for civil rights and civil liberties and this incredible intrusion into our lives and our communities?

Nicholas Bustamante 34:36

I think that again, this is one of the problems with the Fourth Amendment or privacy law generally, is that you know, once you go out in public, you don't have an expectation of privacy. I think that that should there should be a reframing of that to have a right to anonymity and public have a right to Association under the First Amendment, but that is it It's a huge problem. And I mean, Project Green Light was one of the first well documented instances of that I think later on after the Detroit model, New York installed a similar model to have all of these images captured and go and go through one of their data command centers there. And this isn't just this goes on and on, along with every every major city law enforcement uses facial recognition, to document and track movement of people to document and track movement of traffic to document and predict criminal behavior. Um, I think that, I think Amazon got a lot of flack, and rightfully so for the recognition software, which was exposed to misidentify Black members of Congress. And first, first and foremost, it's good to know that one, Amazon is not the only company that develops and deploys this software. So it's good that it is that attention was drawn in to that software. The software's are available from other tech firms, and they are purchased and used by law enforcement. And they are used that ports of entry they are used at the border. The problem with misidentifying people is that what it's it's abhorrent, especially if it's going into a criminal offense. And the the response to that is well, why don't we just put more people of color into the database then, so that these systems can better identify people of color, because there isn't a well documented error rate for people who are have a darker phenotype. But the, that, to me only doesn't really address how they would be deployed against those communities and how they're being used to predict or model big data to predict crime. And where a local law enforcement would put its resources based off of those predictions, I think, ultimately could lead to more police presence in communities of color. So I think that any going to Dr. Quan's point about addressing bias in big data and artificial intelligence, smart algorithms, addressing the error rate for how it identifies people is kind of a drop in the bucket concern to me. And the primary concern is well, how is this data being used and coded to potentially be used against people of color. And there was a really good piece that was done in I want to say pro publica. And they documented the use of a and a probation are a risk assessment associated with people who were convicted of a crime. And they would be sentenced within a range based off of that of an algorithm that was used to assess their likelihood of re offense or their risk associated with their criminal charges. And what that what their piece found was that the COMPAS system was, it was being used in a local court to assess people's risk. And what happened was, is that time and time again, black and brown people were more likely to receive higher risks associated with their score than where their white counterparts, including white counterparts who had more criminal violations, or criminal convictions rather. And I think that the ACLU is involved right now in ongoing litigation, on the use of a similar type of algorithm in detention centers, where there's an assessment risk associated with a detainees release. So me in any addressing of bias, it has to go beyond just the the issue of people that are going to be misidentified. What concerns me is that how people are going to be identified within the parameters set by that algorithm.

HLT Quan 39:42
Yes, thank you, especially since as Wired Magazine reported recently that the best algorithm available continue to misidentify black people something at a rate of five to 10 times higher than they would white people. So your point about the error rates is well taken. Tanner has questions. I know, we also don't have a lot, a lot, a lot of time left. But at some point, I do want you to come back and, and and answer the question. If error rates is not where the solution lies, what is to be done? What are the solutions? What are the things we should be concerned of, but um, I'm gonna let tanner go first. So go ahead, tanner.

tanner menard 40:23
Thank you, Dr. Quan. And thank you so much for all of this information, Nick. I have a similar question to Dr. Quan, which is just, you know, we're learning about the extent to which we are surveilled, and how powerful the technologies are that are being deployed, basically against us. So once once we start to demystify these things, like, once we start to get past the myth of Big Brother and to actually look at who is behind the curtain, what, what are they actually doing? What steps can we take as citizens? And how can we organize to reclaim our right to data to our data like to like, how can we demand for instance, that we know when we're being surveilled? Or that we understand that we be told the conditions of algorithms that are being used to surveil us is, how do you propose that we start to gain agency over these systems?

Nicholas Bustamante 41:37
I think a good first step is by organizing to pass laws in local state legislatures that require whenever these systems are used, particularly in the criminal justice context, that they're audited for racial bias and gender bias and class bias. I think that um, another issue is to pass stronger state or federal laws for privacy, particularly as it relates to issues outside of criminal justice, because there, you could going to Shoshana Zuboff point, the Fourth Amendment is so limited. And then data that is coming from the consumer perspective, consumer sector can easily make its way into the criminal justice sector. And people should have a right to know how in what way their data is being monetized. Some people have suggested people to be paid for the data that they use. I'm not necessarily that that addresses the problem head on. I think that the goal is for people to start having conversations and organizing around what do we mean when we talk about, about privacy rights in a data, an era driven by Big Data?

tanner menard 42:58
Yeah, I agree. I mean, it's something that I've really been thinking about. My interest in surveillance started around the time of, well, I mean, really 9/11 but when Standing Rock happened I got really interested in facial recognition technology, because of the way it was being used at that particular action that was taking place. And around that time, I think it was a couple years before that, that Facebook started automatically tagging photos. So I did this little project where I would, I studied how facial recognition technology worked. And I started pixelating my selfies in the different quadrants. To the end, the goal was to see if I could produce selfies that Facebook couldn't tag. And it eventually figured out what I was doing and started tagging me as any pixelated photo that I would put into it. Anyway, I wrote I wrote a little book around that. And what what occurs to me is that maybe we need to start thinking about asking for, and I mean, this is purely a conjectural thing. But it seems to me that like in this age of artificial intelligence, we have an emergent part of ourselves that we need to have a right to, and that emergent part of us is anytime we are exposed to some kind of artificial intelligence that analyzes our biometrics our dispositions and our likes, that we, it seems, I mean, like as a citizen, I would like a right to that emergent part of me, and I'm just curious what how people feel about like, how can we organize around that? And that is a question that I think not too many people have really figured out yet. But um, anyway, I just thought I would mention that and see if anyone had something more to say about it.

Nicholas Bustamante 45:14
I think that that it would be great if we were able to put that into the lexicon of, you know, if we're talking about body sovereignty or body autonomy, and have our data be an extension of that, that would be a great first step in changing how people view their right to privacy in the modern age.

HLT Quan 45:39
Yes, indeed. So I know, you know, I ask this question all the time. Are we our data? And are we just our data, or are we more than our data? But and and I know that you always want to ask the question, what is the relationship between data and and who we are as human? So I know you've raised a number of issues today, and I'm just so deeply appreciative of you taking time out from a very, very busy week to talk with us about this. Are there things and issues that we haven't brought up or race that you would like to add? And also, before you answer that question, as a final thought? I wonder if you could comment briefly, though. How are other countries addressing? So either the EU, or China for that matter? Or people in the global south? How are people coping with this differently than we are?

Nicholas Bustamante 46:43
I think that you guys hit everything on the head and what people should be paying attention to, I would draw people's attention to the role that algorithms play in the criminal justice system as another good thing to follow. The EU a couple of years ago, passed a privacy law that basically says that people have a right to be forgotten. And they can be taken off the internet. I think that that's a good starting point. I think California passed a similar bill. And California may have passed or they were talking about passing a bill that pays people for their data. I think that the, I'm concerned with moreso, yeah, I think that people should have a right to be forgotten, I think that people should have a right to being understood as more than their data. I think that the thing that concerns me more is passing laws that subject the companies that are creating these algorithms to a type of auditing system where they're audited for racial and gender class bias, because the fear for me is still that how people are being viewed in light, and through the lenses of these algorithms. That is the primary current concern for me. In regards to what China is doing, I really haven't followed that as much as I should I know that people have organized against it. I think that their social rating score is particularly has a potentially particularly dystopian, but I also don't know how far away we are from that in the United States. So that I, I don't know what people can do other than organize, and have conversations that challenge what we think is private and fight for the piece of ourselves that we want to keep.

HLT Quan 49:00
Thank you. On that note, tanner, did you have anything else for Nick?

tanner menard 49:04
No, I don't. But I just want to thank you so much for the work that you're doing. I think it's incredibly pioneering. And I'm so grateful to you for sharing your knowledge and your research with our audience at Equality Arizona, and Dr. Quan, as always, it's so wonderful to get to work with you on this project. I've really learned so much from you. And I know that everyone out there is just really benefiting from the perspectives that you bring here. Thank you for bringing our first guest to this podcast. And with that, unless anyone has something else to add, I think that that's probably a wrap.

HLT Quan 49:50
Yes, it is. Oh, I would just say to please tune in next month for a conversation on rise of authoritarianism and the right wing policy workshop.

Michael Soto 50:04
This has been a production of ality Arizona. Find us online at equalityarizona.org.