Whose Streets? Our Streets! with Rebecca Williams

Thu, 10/14 12:38PM 33:48

SUMMARY KEYWORDS

surveillance, harms, cameras, people, technology, smart cities, city, collecting, report, privacy, kiosks, data, facial recognition, oversight, identify, san diego, project, police, clause, smart

SPEAKERS

Greg Lindsay, Rebecca Williams

Greg Lindsay 00:24

Hello and welcome to threesixtyCITY by NewCities, a podcast series delving into the future of urban life. I'm your host, Greg Lindsay. More than a decade after Smart Cities promised to transform the urban realm, it's clear their killer app is surveillance. For example, last summer in San Diego, the San Diego Police Department obtained footage of Black Lives Matter protesters from the smart streetlights that were ostensibly designed and installed for traffic control and air quality monitoring. Following public shock and outrage, the Mayor of San Diego ordered more than 3000 cameras turned off. But they stayed on, no longer collecting footage for the city or for the police for that matter, but for the cameras manufacturers. This is just one example of a whole raft of technologies and actors including cameras, sensors, and facial recognition by companies such as Clearview AI, that threatened to destroy the anonymity of the public realm. We're joined today by Rebecca Williams, a fellow and the author of a recent report on smart city surveillance for the Harvard Kennedy school's Belfer Center for Science and International Affairs Technology and Public Purpose Project or TAPP. Her report outlines steps communities can take to stop harmful surveillance and reassert the public's right to the city. Thanks so much for joining us, Rebecca.

Rebecca Williams 01:36

Thank you so much for having me, Greg. I'm a fan of the podcast. And it's a pleasure to be on.

Greg Lindsay 01:41

Well, thank you. I guess as a starting point. Could you outline the genesis of your report and the entire project? Obviously, surveillance of cities way goes back. I mean, we could trace it back to the Middle Ages or before. But the rise of closed circuit television cameras the pervasive surveillance, what's different this time? How has technology changed it and what it really the threats and the harms to people?

Rebecca Williams 02:05

Yeah, so I love that you kicked off this podcast with the San Diego streetlight camera example because it's such a good nugget with a lot of the issues that we'll end up talking about. But the TAPP project, which you mentioned, where my fellowship was based, the theme of the project is analyzing emerging technologies to make sure that where my fellowship was based, the theme of the project is analyzing emerging technologies to make sure that they're serving the public interests. And it's based out of the Belfer Center at Harvard Kennedy School, which came up to mitigate nuclear harms. So I think about that through line in Belfer Center where we have this new technology that can be very dangerous and how do we analyze it, produce policy that prevents or mitigates harms associated with it. And my pitch was always, I'm not doing nuclear bombs, I'm doing smart cities. So, the inspiration for the project was coming off of like the tail end of many live and virtual protests to the Sidewalk Toronto project in Canada. It had not yet shut down, COVID-19 had not happened yet. The San Diego street light camera event had not happened yet, the protests had not happened yet. But the inspiration for the project was alright, this is an emerging technology, tricking out our urban built environment with so many new tools. What are the harms here? And I'm just gonna do that treatment to it. And then time passed, I got into the fellowship and all these other little things happened. The San Diego street light camera thing and the general themes of surveillance came pretty early on during the pandemic, which reoriented/inspired the research to head in the surveillance direction.

Greg Lindsay 04:05

I love the fact that Belfer started with nuclear because I saw a great analysis once that facial recognition in particular should be thought of as like plutonium. Like it's extremely dirty, poisonous, has extremely limited uses, preferably in deep space. So I want to come back to facial recognition. But I guess first question is in your research into smart cities, at NewCities we started covering this 10 years ago, I was a journalist writing about it then Cisco and IBM and others a Smarter Planet, all this. My question for you is was surveillance always the goal or did they wander into it because so of these other technological promises fell flat or were never rendered? Is surveillance the only business model that worked because of the prevailing institutions in cities? How did we end up here where sticking a camera on everything became basically the way that smart cities got instrumented?

Rebecca Williams 04:53

Yeah, I think a couple of things to tease out of your question, like one does surveillance even work as a business model? What are the business models of smart cities and maybe they're sort of exploring those, the companies that are selling related products. But then at the same time as like the hype of smart cities was coming up over the last like 20 years, like my big fear about smart cities 15 years ago is just cities are being sold a bill of goods, because even if you add a bunch of sensors, our urban problems are so complicated, like people have talked about this a lot. Like you're not going to solve it just with like a particular new data set. And those data set receptors are really expensive. So is that the best way to spend your money? But I was more concerned about cities being sold a bill of goods than surveillance, per se. But as I mentioned, I really explored what are the harms of this as a research topic and ended up with the emerging theme being surveillance after circling it a few times. And I think it's less about the evolution of smart cities hype, or business models, per se. And more about we have this other stuff going on, which is police technology and just general corporate and government surveillance. The San Diego example is quintessential in that they didn't buy the street light cameras to film the protesters. But it turned out there's this other thing going on in society, where some other folks might want to film protesters. And it turns out there was a camera on the street light. So it's not accidental, but it's just more converging then smart cities really found a sweet spot business wise in the United States. I think elsewhere, especially in India, there's a big CCTV facial recognition technology trend right now. And they call that smart cities, like it's synonymous. To the point where maybe they just mean cameras for smart cities in India. And maybe that's a different thing. But I know that they do a lot of things. I'm not sure it's the best business model as it is just sort of converging things in society happening at the same time.

Greg Lindsay 07:28

What is the most pertinent threat when it comes to smart city surveillance? Much has been made of facial recognition, as I alluded to earlier. But what strikes me as different this time is that these devices were never recognition, as I alluded to earlier. But what strikes me as different this time is that these devices were never networked, like Amazon ring for example, is an emergent thing where it's private and unaccountable. The system just gets bigger and bigger and bigger as any individual node gets wired in there, like network effects and surveillance strike me as pernicious as well. So I'm curious, what you identify as the biggest threats to the public and to law frankly as we know. It's one thing when the police do it, it's another thing when private corporations do it without any real accountability.

R Rebecca Williams 08:03

Yeah, so this is my best answer. I don't know if it's avoiding the question. But I think the most dangerous aspect of it is how easy it is to identify individuals at this point with things like facial recognition technology. But by the way, there's going to be a lot of other recognition technology spreading if not this. The thing I kept coming back to was not just surveillance related, but the most threatening parts more if you can tell it is me or being able to track individuals across really creates a new power dynamic. Even though we considered public space as quasi non privacy zones in the past, like people wouldn't recognize you if you walked to the store, unless you ran into somebody knew. So we're changing space as we know it. The other smart city tools that are just picking up temperature, like how many people step on the tile did not make it into my analysis when I was trying to figure out the worst harms. Maybe they're still expensive, maybe they have other downstream effects on the environment, or there could be other things. But the most dangerous thing was attaching things to identity and it's not just for privacy, but for discrimination and for power. One of the harms I characterize is totalitarianism.

G Greg Lindsay 09:36

You really put a point on that one in particular.

R Rebecca Williams 09:42

What are the most extreme harms I could think of with smart cities and I think a lot of very classic, some folks might say alarmist or very extreme language, I think applies. If you create a situation where you're always being watched, and can always be identified by not just the police force or the government state, but corporate entities or even each other. That's why some of the facial recognition technology conversations are so interesting when there's even these spin offs to Clearview AI, like the PimEyes tool where you could conceivably just be out in public and someone could take a picture of you and look you up. It's a completely different space. So if there's one takeaway, well, there's 10 takeaways from the report, but the top one is don't share with police. But the number one takeaway is the identifying data. If we stop collecting or storing or repurposing that, a lot of the harms start going away in my view. Or the most dangerous ones.

G Greg Lindsay 10:48

Well before we get to your recommendations, because you do have some, which is one of the things I like most about your report as opposed to simply categorizing the many, many harms that are being done. One thing I want to talk about is the discrimination aspect. Is that a bug or in fact is that a feature in terms of who these technologies are designed to support? And we've already had cases, for example, where facial recognition has failed to even identify people correctly who have been arrested on erroneous charges based on that. Has anyone even bothered to put together the processes in place to ensure this doesn't happen? It strikes me that there are very much these powerful forces at work, that want to have this kind of plausible deniability that the technology makes possible, versus even trying to rein it in.

Rebecca Williams 11:34

The discrimination aspect to smart city technology, or even just for the cameras and facial recognition technology in public space is really interesting, because it cuts both ways. I tried to get a little bit at that in the report, where I could see it as a tool for targeting discriminated against groups, and that might be different in different countries. But the point again, is if you can identify people, which is what this technology has the capacity to do now. You don't even have to have built in facial recognition technology to the camera, if you're recording images, you can just apply that technology on top. So there's this new affordance in these technologies about identity. So if you're in a society where we discriminate against certain identities, and cameras can pick that up, it makes all of that discrimination that much more dangerous. And by the way, we live in that society. If you feel uncomfortable talking about the United States, maybe you can observe other things happening throughout the world, but so it just makes that sort of discrimination a lot more dangerous. But then to the the flip side, there were some cases that didn't even make it into the report. Some anecdotal stories I've heard about security cameras in different parts of town. I interviewed Susan Crawford for this report. She's done a lot of net neutrality and other smart cities writing. One of the nuggets that she gave me in our first conversation was that in Chicago, when they were installing more cameras around a more affluent group more white people were like, "my civil liberties, stopped filming me." But then when they would ask people in the south side of Chicago, a poorer black population, they would say, "please install the cameras, we have crime and I need the cameras to protect myslelf." And then LinkNYC in New York is trying to fulfill their contract of setting up these kiosks that also have cameras, by the way. But the underlying quiet shadow business model of LinkNYC is they're to sell ads on the kiosks. From the view of the vendor, the more expensive eyes are in certain parts of town. So those kiosks have been installed. But then the kiosks haven't been installed in the less affluent parts of town because it doesn't seem like as good of a business proposition. And they're sorting that out, but it goes both ways, and it ties back to not only identity of discrimination, but also certain parts of town getting certain things. I thought a lot about for example, nicer parts of town getting higher quality cameras, and is that good or bad?

Greg Lindsay 14:33

That's ironic to say the least. Yes, higher resolution.

Rebecca Williams 14:36

So I think it's just something to watch for. But to your point about are cities thinking about this? At least Seattle is. Let's say there's less than 20 jurisdictions in the United States that have things called surveillance technology oversight laws. I did some writing about this in the report and then also separately for Belfer. But they range in how intense they are with their oversight of surveillance technology and Seattle's on the more extreme end, in that they do a lot of oversight. And Seattle has equity impact assessments assigned as part of analyzing, should we use anything that surveils people? But the law has been in place for a few years, and they have some of these impact assessments online. And when you read them, like I did, there's not really anything to them. It's like, well, we did some analysis and we're not really sure how this affects equity. And that's the best example I have for this stuff right now. And I know, some other cities are exploring equity impact assessments for other sectors or issue areas. DC is trying to do it for like a lot of things, not just surveillance technology. And it might be in vogue as like a new policy scheme. But I couldn't find satisfactory government oversight of these things in that realm. And I had started to see some journalism that tried to highlight, well only this part of town has this traditional urban planning, which neighborhoods get what type of analysis. But nothing seemed very rigorous to me thus far.

Greg Lindsay 16:28

Speaking of rigor, you lay out recommendations in the report and I would love for you to walk through them quickly. They're grouped into three categories: one, stop doing harm, second, figure out how we can evaluate these technologies in general to put some teeth into it, and then how to build that up. I'm curious, can you quickly walk us through how to implement them? And has anyone done a decent job of it? Does anyone have any teeth in these kinds of oversights?

Rebecca Williams 16:54

So to dive into the behind the curtain of the research, which is what podcasts are for, when I set out to do the research I wanted to assess cities on like a scorecard, which I thougt was going to be possible and useful. I thought there was a lot of emphasis at the TAPP project, they hire practitioners versus traditional academics, because they're hoping to produce research that folks could actually walk out and apply. So like more applied research versus just theory, which I think is good, especially in the technology space, because folks need tools. Like when I talked to city governments, they were saying, we just need to know what to do and we need a network to talk about this. I kept hearing these same things when I talked to city officials. One of my hypotheses was that I was going to come up with some contract language. So just like a snippet of contract language, what could be more practical than a clause, when you're procuring things, we'll put in a clause. And then as I was doing the research, I couldn't find the perfect clause that would fix all these problems, one. Two, there's not a lot of incentive the way business dynamics and procurement work for some of these clauses to go through. And then as I was analyzing some of the things that play in the policy space like the surveillance oversight laws as well as some privacy laws, and since things kept spilling over into like police tech some things related to that as well. I didn't come away from the research thinking this is perfect do as Seattle does, because like I said, I opened the Seattle reports and thought it didn't really seem complete yet. But it does seem like Seattle is better than a city that is not doing anything. The flip side of Seattle too is I heard that it was a lot of overhead and a lot of work to get anything done. There are a lot of reasons that I wouldn't call out a best practice and do this. My recommendations started getting around stopping the identifying data stuff because there really just is no policy framework right now for if one department collects it, can it end up with the police? And I thought the police was a pretty severe harm based on the examples that I was collecting for the reasons stated. So it seemed like to define a priority, let's just set up some policies where that's not automatic. Maybe you need a warrant for that. Maybe you don't collect that. These are options that do exist. And then the next two sections deal with, we've been using this emerging technology without any regulation, I've identified some issues, so we've got to stop these really extreme things. I started off examining smart city harms and technology harms and privacy or whatever else and at the end of it, I became almost like a democracy stan, the internet term. If I wasn't already, but tech is very authoritarian by nature. I don't know if it's intrinsic, if other people have made these arguments, but standards, efficiency, and one person in charge, it really lends itself to like some of the big words I use like "totalitarianism." It really scales that well, and it's not super democratic. So a lot of the stuff I was coming back to was like, how do we re-up democracy with technology? Considering that right now just autopilot technology seems to be getting more and more authoritarian. So I think we need interventions to make sure that whatever we're using is more democratic. So that's what the other two sections became about. Building that capacity to have conversations about it, to test it. Not that there was a perfect answer, that all of a sudden, if we turn these things off, everything would be good.

Greg Lindsay 21:02

How do we build that capacity? I mean, to me the most interesting thing about the San Diego incident is that there was in fact public outrage about it. So much surveillance technology is simply written off as "creepy" and there's a waving of hands in the air, there's not much we can do about this. For example, Amazon ring runs television ads, or compiles footage that is taken without permission from people's homes and porches, and used to do cute post-Halloween things. And, no one even raises the fact that that's a gross violation of their own privacy. That level of surveillance is just accepted. How do we as a starting point even, build the recognition that this is unacceptable, that this is introducing harms? Because, at best people are fans of this tech. Ring preys on a baseline American paranoia about the public realm. And, even at worse, people see it as helpless, just as something that's part of policing. So, what are the levers that activists or even concerned city officials, who want to rein in or put an oversight on this, where can they build power or build leverage points?

Rebecca Williams 22:10

I genuinely believe in these recommendations, but I know they sound like the recommendations for everything. We need more transparency to what's going on, we need collective action. My whole hope for this report to the extent that it was useful other than me doing a deep dive during the pandemic, like a fever dream, was to make sure that I had as many examples as possible. So it was not just rhetoric versus rhetoric conversations, but demonstrate some examples of that going wrong, and do you want that or do you not? But always working off of real life example. So I think, as members of our democracy have a lot on their plates, there's a lot to worry about. So I think to the extent we want to worry about smart city technology, it's important for urbanists and folks that might listen to this podcast to just make sure that we are spreading the harms far and wide. One of the things that I observed in some of these conversations is you have digital advocacy folks over here and transportation planners over there. And they don't really hang out together very often. So I think another thing is connecting groups and making sure that they're talking about digital rights and issues at the transportation conference. That has to be a panel forevermore if we're doing all of this tracking. I saw transportation as a very vulnerable spot for privacy and I see it as probably the future of a lot of fourth amendment case law with the license plate readers and all these sorts of things.

Greg Lindsay 23:52

I think it's funny you mention that because NewCities and our sister arm CoMotion, we're planning our LA event and the Los Angeles Department of Transportation invented their own software standards for monitoring this tech, which has been the subject of federal lawsuits by the Electronic Frontier Foundation. It's funny, Selena Reynolds, who runs LA Dot has countered in a way that, if you think what I've created is bad, she argues, you should look into what tolling collects in terms of capture of license plate data and how those datasets get integrated. There's a lot of leaky data sets who would appear to be in government that perhaps we need to firm up first.

Rebecca Williams 24:28

I went to school for law and city planning and I worked for a regional planning association as an intern back in the day, before I got into data stuff. So I have some background in the planning world, but I'm probably more digital advocacy nowadays. But I'm not unfamiliar with transpo subcultures and things. I sympathize with these transportation systems that have been collecting data forever, like what's the big deal now? And the big deal now is that it's so much more and you can identify people and that's different. You could have before, but at some point when you scale these things, or they become so efficient, you have to rethink what the rules might be. There might be planners that are watching this now, thinking about a lot of the drama that's happening with census data and privacy, which is maybe not the best example of changing the rules. But an example of where we used to provide all this census data, and then we realized that you can identify people, so now we're gonna do a different set of distribution. Maybe you have to fill out a special report to access it. Is that good? Did you just destroy the utility of so many people? I think this is the conversation that transportation planning also has to have. And I'm not sure the census solution is the best solution, but we just need to recalibrate. The point is things have changed. Recalibration must happen and so we should be discussing things on the recalibration layer versus just keeping things the way they have been.

G Greg Lindsay 26:12

I want to come back to one last point, you mentioned procurement earlier, and writing procurement contracts. Which I thought was a really interesting way into this, because so much smart city tech really is this nexus of private industry procurement contracts and how governments don't delve into this. I'm curious your thoughts of how we could reform that process in terms of building the capabilities for cities to even understand what it is they're provisioning and protecting themselves in this way. Because this has been the movement of the open source software and cities starting to figure out how to build technologies themselves, like LA did in that particular case. Is there a legal way out of this in the sense of putting those safeguards into place and perhaps clamping down there? Where's the choke point here, procurement strikes me as one without having to get into messier discussions about policing and things if you could basically put in some ironclad clauses, but it seems like that perhaps is a bit utopian.

R Rebecca Williams 27:04

A couple of things come to mind when you asked that question. One, I think cities are in a vulnerable position, often as a buyer, maybe with all things, but certainly with technology for a variety of reasons. I think it's very expensive and the budget cycles are complicated. I think the contracting officers aren't always data or software experts, because they're contract experts. So certain clauses might not occur to them as downstream effects. But also, when I was talking to folks, Link NYC renegotiated their contracts several times after outcry about privacy, and they change their privacy policy, and all these things. But I think they were able to do so because it was New York City. As I mentioned, the shadowgoal of that project was these advertising dollars. The billboards in the kiosks around New York City are worth more than in a smaller city, so maybe it made sense for that project. But other smaller cities don't have the same buying power to say, you're not going to control any of the data for a secondary market, and we're gonna lock it down for whatever, but you're going to be getting this other good. Like, I think the business models are a big part of it. Another big part of it, that became clear when I was talking to city officials is they don't know who the subcontractors are of a lot of these projects. So they'll purchase something from, I'm using this as an example, I don't know if it's exactly correct, they'll pay for Panasonic insights and then Panasonic will buy data from data brokers. The Markup just did a great expose on a bunch of companies that take location data from your phone, remix it, and sell it. One of the places they might sell it to is like a Panasonic. So there's this whole stack, but it's not even visible to a government contracting officer that they're collecting that. So governments can be in a position where they're unknowingly or inadvertently promoting this market system that does threaten your privacy, when they just thought they were buying insights. So I think a lot of it is transparency and needing laws at every level. It can't just be the contracting officer. That's where the clause wasn't satisfactory to me. It also has to be like, we can't have these data brokers on phones and it also has to be X and X and a lot of these companies will just not contract, they'll give you the first year for free and then it doesn't go through any of those oversight laws I mentioned. So there's a list of five things you need to actually make sure you have the same privacy or data licensing principle to and if you're only doing it at one, you're gonna miss the other.

G Greg Lindsay 29:54

You mentioned earlier that when you were compiling this you wanted to collect as many examples as you could. And during your reporting on this, you publish a weekly newsletter that chilled the blood, you had so many examples to show how this was all piling up. The reports published, but going forward how are you continuing this work? Are you thinking about restarting the newsletter? Are there other resources or groups that are really pushing this forward that listeners could go track down if they want to get more involved with this issue?

R Rebecca Williams 30:17

R Rebecca Williams 30:17

Great question. As far as the newsletter, it remains to be seen if I formalize that in some way, it's been several months now so maybe that will not happen. But in the recommendations, I tried to include groups that you could join either as an interested community member or just other orgs. to follow. Again, just citing everything like, these are all the groups, these are all the examples. In terms of my work going forward, I'm doing some freelance work right now related to Fourth Amendment privacy stuff, some related to smart cities. One is a phone project, the other is potentially a street light camera project. So I'm doing more legal research and then hopefully in the future I'll get back into digital identity management, again, another vertical of identity issues. But I think that there's a lot of digital identity work that goes unnoticed, because it's just to sign in to applications, but that they will soon be, if not already, connected to some of these more punitive state surveillance type of mechanisms. And I think that's a danger of our authoritarian future. And if I want a democratic future, I think it's very important to think about how that information is collected and used.

G Greg Lindsay 31:42

Absolutely. We may as individuals be done with things like Facebook and the smart city, but Facebook and the smart city are certainly not done with us when it comes to compiling those data profiles. Well, thank you so much for joining us, Rebecca. This has been a fascinating conversation, a bit of a wicked problem. I was hoping that you could solve this for us in 30 minutes, but it seems like more democracy is a recommendation that is a hard one to execute. Thank you as always listeners for joining us, and we'll be back next week with another episode of threesixtyCITY.