Russell Squire
Chair

Will Brightbill
District Manager

505 Park Avenue, Suite 620
New York, N.Y. 10022-1106
(212) 758-4340
(212) 758-4616 (Fax)
www.cb8m.com – Website
info@cb8m.com – E-Mail

The City of New York
Community Board 8 Manhattan
Social Justice Committee
Monday, May 24, 2021 – 6:30PM
This meeting was conducted via Zoom

Please note: The resolutions contained in the committee minutes are recommendations submitted by the committee chair to the Community Board. At the monthly full board meeting, the resolutions are discussed and voted upon by all members of Community Board 8 Manhattan.

MINUTES

CB8 Members Present: Lori Bores, Alida Camp, Sarah Chu, Saundrea I. Coleman, Rebecca Dangoor, Takako Kono, May Malik, Peter Patch, Rita Popper, Rami Sigal

Resolution for Approval:
Item 1 – Surveillance Technology

1. **"Scale and Scope of Surveillance Technology" presentation by AI for the People, Cornell Tech Digital Life Initiative, Public Advocates' Office**
   Speakers included:
   Mutale Nkonde, CEO, AI for the People
   Dr. Meg Young, Cornell Tech Digital Life Initiative
   Phillip Ellison, NYC Public Advocate's Office
   a. **Ban the Scan film**
      i. The presentation opened with a showing of *Ban the Scan*, a short film on local advocacy by the Brooklyn Tenants' Association who organized against the use of facial recognition technology in their residential buildings.
      ii. The film is about (5:30) in length and can be viewed here: https://vimeo.com/504213380
         1. Additional resources include:
            o Coded Bias film (on Netflix)
            o 60 Minutes episode on Facial Recognition (5/16/21 episode)
               • Note: 60 Minutes omitted Black women scientists who discovered and raised awareness about racial disparities in facial recognition technology: Joy Buolamwini, Timnit Gebru, and Inioluwa Deborah Raji
      iii. Ms. Nkonde described three wrongful arrests by facial recognition technology (FRT). FRT program misidentifies people with darker skin 40% of the time and a "strong" FRT program has 1% error rate. Additionally, she described Clearview AI and a new analog called "Chad" that uses photos scraped from the internet and social media for facial recognition purposes. FRT is only one among the many type of surveillance technologies that NYC is using in its Safe Streets plan.
   b. **What is happening across the country?**
      i. Research consensus on ban on FRT for two reasons:
         1. FRT profoundly underperforms on BIPOC people, especially Black people, and especially Black women.
         2. Even if more accurate, surveillance technology erod privacy and the practical obscurity of everyday life.
   c. **Local Government Algorithmic Equity Toolkit developed by ACLU-WA (Seattle, WA)**

      i.   Dr. Young described the development of the Local Government Algorithmic Equity Toolkit which is available here: https://www.aclu-wa.org/AEKit

     ii.   The City of Seattle has a local social ordinance that any surveillance technologies used by the government must be disclosed to the people. In 2017, with the BLM movement, it was discovered that police were using social media surveillance which was not being reported under the surveillance ordinance. The police considered this type of surveillance technology as "software" and not hardware and didn't fall under surveillance ordinance.

    iii.   City had not considered issues of bias in surveillance technology and didn't think that AI technologies needed to be addressed because they were still "emerging." Advocates sought to overhaul the law.

    iv.   CB8 has a civic role to ask lawmakers questions to make sure that civil rights are being protected. List that distills all the questions that you bring into a representative.

          1.   Are these systems accurate?
              o   Are they robust?
              o   Do they work for everyone?
          2.   Can injustice be perpetuated if they work well?
              o   How does that intersect for racism, sexism, or other protected classes?

d. **Public Advocate's Office Action**

      i.   Mr. Ellison shared that the Public Advocates' Office joined the Ban the Scan coalition with Amnesty International, immigration groups, and other grassroots local advocates.

     ii.   The Staten Island DA's Office was using Clearview AI, a vendor that circumvented the rules. Where is the accountability in the oversight for DA? Who is policing the police?

    iii.   There is a relationship between the private sector and the police. The tech sector's mantra, "Move fast and break things" means not thinking about impacts on BIPOC communities which is exacerbated by not including BIPOC people on their teams and boards.

    iv.   Community boards have a role as they come out of a push to make the Mayor's office more accountable.

e. **Question and Answer (questions and responses paraphrased/summarized)**

Q: What is the status of big tech?
MN: Clearview AI is the most famous vendor because they used social media to get around the database issue. The FRT system in Detroit was called Mark1. Police departments are using various different FRT vendors because of the business model - these vendors often have given technology to government agencies on trial, market to police. Researchers like me don't know they are in use because if it isn't being paid for, it doesn't show up in the government docs. Tech companies want scale. They want to gather data as much as possible so they can sell it. Tech built for and by a white populace, don't have design insights that understand that within a week, a Black woman can have different hair styles and is still the same person. The 2nd Circuit has said that Stop and Search is a violation of our civil rights. Surveillance technologies are an unsubstantiated search.

Q: What is the state of surveillance technology legislation?
MY: There is a push to ban FRT in many places. Portland, OR, has banned both government and the private sector use of FRT. ACLU has led a push for broader police surveillance community control, disclosure of technology being used, assessment of impact, and for either moratoria or bans.
PE: CA issued a 3 year moratorium on surveillance and body cams, MA cities have banned FRT, NY has 20+ local and state bills pending. Biometric surveillance includes gait, face, fingerprints - a host of what can be recorded. Tech and Innovation hubs are the communities leading the ban. Surveillance has historical roots tied to slavery in NYC lantern laws. FRT affects LGBTQ+, trans communities disproportionately as well.

Q: What is the state of NYC/NYS? If there is a 40% error rate - that is close to the flip of a coin. Even if it gets to 5% - even 1% - given of arrests, that's a lot of people.
PE: There are connections of historical and racist surveillance practices to contemporary approaches. What is so alarming here is that the government is using it on protestors to curtail 1st Amendment rights. Congress is looking at how USPS used FRT on protestors and that data is shared with DHS - all this data is shared. NYPD is working with Gentech that is connecting private cameras across the city to create a massive network of cameras. We need

at a baseline to think about how data is being shared and who is sharing it.

Q: Intro 1760-A would ban key fob swipes into NYCHA buildings. The key didn't work 40% of the time and collected the data on when individuals go in and out. Someone has that data. A year ago, congestion pricing task force met and discussed what to do about the data from those cameras.
MN: As a computational social scientist, I look at these questions. For example, license plate reader (LPR) data is shared with ICE. There are major ways - LPR, fingerprints, biometrics - collected locally is shared for immigration purposes. It was how they were filling detention centers.
MY: We need to ask questions about who gets data. There are sometimes good mission driven data collection. We need to restructure how we design these systems.

Q: The right to privacy is very shaky. There are deeper issues of social justice and access to data. Relying on tech v. witnesses can cause complications. Real life situations [describes story about a teenage boy accused of sexually abusing a teenage girl who was eventually cleared because all the surveillance footage from the course of the evening were provided as evidence.] The police were not forthcoming with the evidence and the defense needed subpoenas. How do we make sure that tech is used to exonerate?
MN: I worked on this question in 2017 - Legal Aid Society was thinking about using apps to make sure that poor defendants weren't being held without charge for longer than usual. They used a closed data loop - gathering data around arrest date and charging - once the person was seen and moving through the system. Once they were able to secure a person's release, the data was destroyed. There is no business model for closed data sets. We are still thinking about how data and technology can be used to exonerate and I am still working with Congressmember Yvette Clarke, senate partners, and the Congressional Black Caucus on the No Biometric Barriers bill. Congressmember Clarke brought a case of a Black member of her district who was killed by police. She asked the City to use their technology to look for vulnerable people to help instead of using it to criminalize. We have agency, this could be used for social justice ends, but we have to demand it.
MY: An important distinction between use of cameras and FRT. FRT can be used on any camera. Once information is captured and new inferences are introduced, it produces datafication. Body cam footage raises the same question - is it for surveillance or accountability? Different rules are put in place to think about the policies that need to be put in place.

Q: NYCHA landlord key fob bill passed. We need to ban reverse search warrants and regulate ownership of data. How would you like us to use this information?
PE: There is a resolution to call on reso call on NYC to stop reverse search warrants.

Q: In public we can be videoed and tracked. It can be different because the EU takes a different approach - it doesn't have Citizens United and privacy is a right.
MY: Even if it feels like private sector use seems like the horse has left the barn, the government has a monopoly on use of force. Governments can show up armed and cause physical harm. Getting the government right is achievable.
MN: We can reimagine, reappropriate, and recreate - the laws that exist don't serve us. The EU has the General Data Protection Regulation (GDPR). In IL, Clearview AI was forced to pull out of IL because of privacy laws. Remember the 1st amendment protects our right to criticize the government, not for companies to take and weaponize our data. I published this in the Harvard Kennedy School Journal of African American Policy. Even when you don't have the money, organized people will win out on money any day.

Q: What can we do with state legislation and ballot initiatives?
MN: We need a dual strategy. There is a state level ground game. AFP is looking at S79 - while it bans police use and creates a commission, there is an opportunity to sunset. It is more of a moratorium. We've expanded our ideas of what is possible. I sit on a commission in MA with manufacturers, the FBI, CIA, and ACLU. State strategies to be more aggressive. Develop a better bill and expand beyond FRT to other classes of tech beyond biometrics such as LPR, Shotspotter, and geofencing. You can also work block by block - community by community. I've worked with Senator Ed Markey for 5 years on an Algorithm Accountability bill and impact assessment.
MY: Different jurisdiction responses gives us a natural laboratory - look to the CA legislature to be thoughtful about what is working. There is a consensus that bans are important for certain classes of tech.

MN: AI for the People has commissioned a set of posters with For Freedoms and Joe's Pub for the month of June to get people to start thinking about this.

Q: Was the man from Ban the Scan the same person who was on social media while surrounded by police?
MY: Yes, Derrick Ingram of Warriors in the Garden.

Resolution

WHEREAS, we live in a technology infused society where the collection of data is inescapable,

WHEREAS, this technology includes and is not limited to AI and algorithmic technology which discriminate against people of color, women, LGBTQ communities, those with disabilities, and other protected classes of people,

WHEREAS, research has revealed this technology to be inaccurate and the root cause is structural and not easily cured,

WHEREAS, even if this technology was more accurate, it would not remedy its violation of privacy, human rights conventions, and exacerbate disparities in many reaches of society,

WHEREAS, there is an asymmetry between procurement processes that blur the lines of government and put power in the hands of commercial entities that are not prioritizing the community good,

WHEREAS, S79 and the federal Algorithmic Accountability Act introduced by Congress Members Clarke and Pressley raise the needs for algorithmic justice and are important starts,

WHEREAS, before being fully proven, surveillance technology is field tested in society for law enforcement, social service, and other purposes which has serious justice consequences,

BE IT RESOLVED, CB8 calls for our city and state legislators to take action to regulate algorithmic and AI technologies such that:
1. We can reimagine, reappropriate, and recreate how we use technology in our city and state government,
2. Any bills implement community-based regulation as the checks and balances to ensure that the government application of technology - which interacts with us and extracts data from us - are functioning in accordance with our values,
3. The practice of examining algorithms and AI systems for bias must be operationalized through justice and equity impact assessment PRIOR to implementation,
4. Technologies that exacerbate disparities for the members of protected classes under Title 7 of Civil Rights act of 1964, and biometric surveillance technologies such as FRT, gait, etc., should be banned.
5. Regulate the afterlife of the technology such that continuous efforts are made to regulate data collection so that only minimal and necessary data is collected; that it is secured when in use, destroyed after use, and the public notified when data is shared across City and State agencies.
6. Establish regulations and enumerate the principles we hold dear and hold vendors and companies to these values.
7. Vigilantly guard the commercialization of our personal data and establish mechanisms to redress harm when data is misused.

Motion passed unanimously. In favor: Alida Camp, Sarah Chu, Saundrea I. Coleman, Rebecca Dangoor, Takako Kono, May Malik, Peter Patch, and Rita Popper (Public Member: Wendy Machaver)

2. **Old Business –** None
3. **New Business -** None