STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006

www.StopSpying.org | (646) 602-5600

STATEMENT OF
ALBERT FOX CAHN, ESQ.
EXECUTIVE DIRECTOR
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, INC.

BEFORE THE
COMMITTEE ON TECHNOLOGY
NEW YORK CITY COUNCIL

FOR AN OVERSIGHT HEARING CONCERNING SMART CITIES.

PRESENTED
January 19, 2021

Good morning, my name is Albert Fox Cahn, and I serve as the Executive Director for the Surveillance Technology Oversight Project ("S.T.O.P."). S.T.O.P. advocates and litigates for New Yorkers' privacy rights, fighting discriminatory surveillance. I want to begin by thanking you for the invitation to testify at today's oversight hearing concerning smart cities.

1. The False Promise of Smart Cities

As the world's urban areas are growing, we are many asking how to build sustainable cities. In 2014, John Wilmoth, Director of UN DESA's Population Division, stated that "our success or failure in building sustainable cities will be a major factor in the success of the post-2015 UN development agenda".[1] For many, the answer to the sustainability issue is the creation of so-called "smart cities" – in other words, to increase the use of technology in our urban areas.[2] Supporters of smart cities claim that by integrating the internet of things, artificial intelligence, and networks of sensors into urban neighborhoods, we can collect and deploy data to make our children smarter, our commutes faster, increase sustainability and even save lives.[3] But this is a utopian view of what technology can do for our society.[4] The last few years have time after time illustrated how vulnerable society becomes when we blindly trust that new technology will be better than the systems it replaces and that new tech can be launched without significant testing and oversight. Smart city initiatives promise better urban neighborhoods through data collection. At bottom, this means increased use of surveillance technology, raising privacy concerns as well as the question of physical responsibility.

2. Risk of Governmental Abuse

The risk of governmental abuse of technology is not an alarmist threat of what could happen in the future, it is already happening. S.T.O.P. has time and time again expressed concern for how New Yorkers' basic rights to privacy are violated by the NYPD's growing use of facial recognition and other forms of biometric surveillance. These technologies allow the police to turn a walk down the block into a warrantless search by the use of surveillance system without the need of a court authorization. The thought is disturbing, but it is even more alarming when one contemplates the use of such technology near political protests, health care facilities, an alcoholics anonymous meeting, or anyplace else where New Yorkers have heightened privacy concerns.[5] The smart city initiative would increase the use of these intrusive surveillance systems even further, including, among other things, the implementation of acoustic monitoring technology to measure the noise levels around the city. The privacy impact of such technology is huge; we would practically be only one software update away from warrantless wiretaps of every New Yorker walking down the street.

[1] https://www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html

[2] https://www.mckinsey.com/business-functions/operations/our-insights/smart-cities-digital-solutions-for-a-more-livable-future#part1

[3] *See* Timothy Williams, *In High-Tech Cities, No More Potholes, but What About Privacy?*, New York Times (Jan. 1, 2019), https://www.nytimes.com/2019/01/01/us/kansas-city-smart-technology.html?searchResultPosition=3.

[4] *See e.g.* John Lorinc, *Smart cities will be cleaner, accessible, even more democratic, proponents say. But governments adopting new tech must contend with risks, too*, Toronto Star (updated Jan. 05, 2021), https://www.thestar.com/news/atkinsonseries/2021/01/04/smart-cities-will-be-cleaner-accessible-even-more-democratic-proponents-say-but-governments-adopting-new-tech-must-contend-with-risks-too.html.

[5] *See Statement of Albert Fox Cahn, Esq. Executive Director Surveillance Technology Oversight Project, Inc. Before the Committee On Public Safety New York City Council For A Hearing Concerning, NYPD's Roll Out Of Body-Worn Cameras & Introduction 1136-2018*, submitted November 18, 2019, https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/5dd31d2ee51d1670591b13de/1574116654793/2019-11-18+Body+Cams+Testimony+v+FINAL.pdf.

Surveillance tools pose a privacy threat to all of us, but they pose a particularly potent threat to members of our immigrant communities. All too often, these systems create a risk of information-sharing with federal agencies, including ICE. For example, the NYPD for years has contracted with the private firm Vigilant Solutions, which operates a nationwide database of over two billion license-plate data points.[6] Shockingly, in 2016 we learned that Vigilant Solutions was not just contracting with local police departments, but also with ICE.[7] Perhaps most disturbingly, the NYPD relies on Vigilant Solution's artificial intelligence to map out social networks, label New Yorkers as "criminal associates," and create databases based on the company's unproven algorithms.[8] This is just one example of the governmental abuse of surveillance technology that is already happening in our city. Then consider the exponential increase of data collected and processed in making New York City "smart" – the potential privacy impact of New Yorkers is horrifying.

3. Risk of Abuse by Third Parties

In addition to the risk of governmental abuse of the systems used, and the data being collected is the increased risk of outside threats. The last few years have shown how increased use of technology also makes us more vulnerable, with the Cambridge Analytica Scandal one of the most infamous examples of abuse.[9] Instead of progress we see how technical development often is hijacked by rogue state powers and their corporate enablers. Corporations and unscrupulous world leaders use technology to influence public opinion and democratic processes and institutions.[10] As an example, Vladimir Putin's Russia has been accused of interfering not only in the U.S. 2016 election but also in the UK Brexit referendum the same year.[11] One of the latest examples of a coordinated effort to undermine security measures is the SolarWinds Hack.[12] The hack, which was uncovered late 2020, is suspected to be another attack carried out by Russian hackers. The targets of the attack included U.S. federal agencies as well as large American companies such as Microsoft, and the extent of the damage is still under investigation.[13]

Municipalities like New York City are not spared from these threats. Indeed, we are only one hack away from all data collected being used by those we do not wish to have access to it. The smart city

[6] *See* Rocco Parascondola, *Exclusive: NYPD Will Be Able to Track Fugitives Who Drive Past License Plate Readers Across the U.S.*, N.Y. Daily News (Mar. 2, 2015), https://www.nydailynews.com/new-york/nypd-track-fugitivesdrive-license-platereadersarticle-1.2133879.

[7] The Domain Awareness System collects the license plate data scanned by the approximately 500 license plate readers operated by the NYPD and combines it with footage from cameras and other surveillance devices around the city. The NYPD holds on to the license plate data for at least five years regardless of whether a car triggers any suspicion. See Mariko Hirose, *Documents Uncover NYPD's Vast License Plate Reader Database*, ACLU (Jan. 25, 2016, 10:30 AM) https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-readerdatabase.

[8] *See id.*

[9] *See* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, The New York Times (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[10] *See e.g.* Abigail Abrams, *Here's What We Know So Far About Russia's 2016 Meddling,* TIME (Apr. 18, 2019, 8:20 AM EDT), https://time.com/5565991/russia-influence-2016-election/.

[11] *See e.g.* Patrick Wintour, *Russian bid to influence Brexit vote detailed in new US Senate report*, The Guardian (Jan. 10, 2018, 10:15 EST), https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report.

[12] *See e.g.* Alyza Sebenius, *SolarWinds Hack Followed Years of Warnings of Weak Cybersecurity*, Bloomberg (Jan. 13, 2021, 6:00 AM EST), https://www.bloomberg.com/news/articles/2021-01-13/solarwinds-hack-followed-years-of-warnings-of-weak-cybersecurity.

[13] *Id.*

initiative turns the urban neighborhood into a data collection machine, making New York City even more vulnerable to attacks.

4. Risk of Flawed and Biased Technology

Another issue that needs to be addressed is the technology used in making a city "smart". Artificial Intelligence (A.I.), machine learning, and biometric measuring technologies are used in order to process the enormous amounts of data collected in smart cities. The technologies used are more often than not both flawed and biased.

Algorithmic discrimination through the use of Automated Decision Systems (ADS) is one example of this. Due to the large datasets collected and analyzed in a smart city, ADS offers an attractive technology to simplify decision making while still taking all collected data into account.[14] At a first glance, ADS seem to offer understaffed and cash-strapped cities the promise of efficient, accurate decision-making support. However, while ADS are sold to the public as "objective" and "scientific", they are frequently just as biased as human decision makers, if not more so. Only ADS regularly discriminate opaquely, often leaving victims without any legal redress. Even worse, one biased ADS can impact thousands of civilians, having a far larger discriminatory impact than any one human decision maker could. With built-in bias, the impact of using ADS in such a large scale as an integrated part of a smart city can be devastating. This is especially true for community members already suffering from discrimination.

Another example of flawed technology is the systematic discriminating technology of facial recognition systems. As documented by M.I.T. and Stanford researchers, many commercial facial recognition systems are incredibly accurate for Caucasian men under certain test conditions, but they fail up to one-third of the time for Black women in those same exact conditions.[15] Facial recognition systems have similarly been shown to perform poorly on the elderly and children.[16] The harmful consequences of over-surveillance are well-documented,[17] as is the fact that communities of color disproportionately suffer from its adverse effects.[18] Increasing this type of technology as part of a smart city project therefore could have immense negative effects of the people of New York.

5. Concluding Remarks

When discussing the development of these smart-city initiatives we must ask ourselves if the technology of smart cities on one hand, and a free, democratic society on the other hand may co-exist. The last few years' examples of misuse of technology illustrate how the technical development may be used as a tool to threaten human rights and undermine our democratic institutions rather

[14] *See e.g.* Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City* (20 YALE J. L. & TECH. 103, 114-115 (2018), https://yjolt.org/sites/default/files/20_yale_j._l._tech._103.pdf.

[15] MIT Press, Study finds gender and skin-type bias in commercial artificial-intelligence systems, available at https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[16] Jack Corrigan, *Experts Tell Congress Facial Recognition's Bias Problem May Be Here to Stay*, NextGov, available at https://www.nextgov.com/cio-briefing/2019/07/experts-tell-congress-facial-recognitions-bias-problem-may-be-herestay/158320/.

[17] *See, e.g.*, Carlos Torres et al., *Indiscriminate Power: Racial Profiling and Surveillance Since 9/11*, 18 U. PA. J.L. & SOC. CHANGE 283, 299–300 (2015).

[18] *See, e.g.*, Barton Gellman & Sam Adler-Bell, Century Found., *The Disparate Impact Of Surveillance* (2017).

than improve people's lives. We must not only look how the technologies are supposed to work but also how they may be abused. After all, New York is not a computer, it's a community. [19]

[19] Shannon Mattern, *A City Is Not a Computer* ,Places Journal (February 2017), https://placesjournal.org/article/a-city-is-not-a-computer/.