ACLU of New York

Legislative Affairs
One Whitehall Street
New York, NY 10004
212-607-3300
www.nyclu.org

Testimony of Daniel Schwarz

On Behalf of the New York Civil Liberties Union

Before the New York City Council Committee on Technology

Regarding the Oversight of "Smart City" Technology

January 19, 2021

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony regarding the oversight of "smart city" technology. The NYCLU, the New York affiliate of the American Civil Liberties Union, is a not-for-profit, non-partisan organization with eight offices throughout the state and more than 180,000 members and supporters. The NYCLU's mission is to defend and promote the fundamental principles, rights, and values embodied in the Bill of Rights, the U.S. Constitution, and the Constitution of the State of New York. The NYCLU works to expand the right to privacy, increase the control individuals have over their personal information, and ensure civil liberties are enhanced rather than compromised by technological innovation.

At its core, "smart city" is an umbrella term covering a wide range of urban surveillance technologies. As sensors and software increasingly merge our digital and physical environments, and new forms of data collection, analysis, and automated decision-making are deployed in our public environments, we are crossing a tipping point. Networked devices throughout the City allow for the invasive tracking of practically every New Yorker's whereabouts and associations – even identifying activists at protests. And software tools make invisible decisions impacting people's fundamental rights in welfare, education, employment, housing, health care, the family regulation (or child welfare) system, and the criminal legal system.

In the absence of meaningful privacy legislation at the state and federal level, we will continue seeing the adoption of new technologies that don't meet people's needs and invade their privacy. We urge the Council to create safeguards and regulations to ensure our civil rights and liberties are protected. This means increasing transparency and oversight as a baseline requirement, severely limiting data collection practices, banning discriminatory technology, and

providing equitable and safe technology access to those in most need. New Yorkers should see their lives enhanced by 21st century technology, not become victims of it.

Introduction

The term "smart city" is a catch-all for a wide range of technologies and initiatives in urban areas. The phrase first appeared in the 1990s but wasn't popularized until various product marketing campaigns adopted the term around 2008, when technology companies began to sell the promise that "smart city" devices and projects would make cities cleaner, safer, more convenient, more efficient, and ultimately improve residents' overall quality of life.

Broadly, most "smart city" technologies fall into two categories: (a) one or more networked devices that collect and share data; or (b) tools, including software, that process or analyze data and act on it by making or supporting decisions. They fundamentally exist to harness massive amounts of data and are therefore drivers of urban surveillance, which will be the primary focus of this testimony.

Urban surveillance technologies create, collect, process, share, or analyze vast amounts of real-time data (from sensors) and historic data (from city agencies or third parties). Some, like cameras and audio sensors, are easily identifiable as surveillance technologies, while others, like WiFi routers or smart meters may not at first glance appear to collect or use personally identifiable information. As traditionally siloed[1] personal data are shared across collection systems and new types of sensorial collection are deployed, the risk increases that previously innocuous datasets will be combined and analyzed in ways that threaten people's rights, liberties, and safety.[2]

The dangers don't lie in just data collection: the underlying algorithms that apply the data as part of an automated decision-making system are far from perfect.[3] Researchers and experts consistently reveal their inaccuracies and biases. Many studies have challenged

---

[1] A data "silo" is an arrangement wherein only one group of people have access to a certain data set. Data silos can be useful in protecting sensitive or classified information, or harmful if faster information sharing is necessary.

[2] *See e.g.:* Ben Green et al., *Open Data Privacy*, BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY RESEARCH PUBLICATION (2017); Kathleen McGrory & Neil Bedi, *Targeted. Pasco's sheriff created a futuristic program to stop crime before it happens*, https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing (last visited Jan 19, 2021); Jeremy Gorner & Annie Sweeney, *For years Chicago police rated the risk of tens of thousands being caught up in violence. That controversial effort has quietly been ended.*, CHICAGOTRIBUNE.COM (2020), https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html (last visited Jan 19, 2021).

[3] danah boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon*, 15 INFORMATION, COMMUNICATION & SOCIETY 662–679 (2012).

algorithms' opaque or "black box" operation [4] and provided evidence of harmful, [5] discriminatory,[6] sexist,[7] and racist[8] outcomes.

Risks and Harms from the Proliferation of Unregulated Urban Surveillance

It is virtually impossible to participate in modern society without leaving a trail of data. And our contemporary "smart city" environment collects all of it, ensuring that each interaction and transaction in our public places can be logged, shared, and analyzed.

Installing ostensibly benign "smart" products like recycle bins that send notifications when they need to be emptied, or streetlights that adjust their brightness dynamically, are often the first step for cities looking to embrace "smart city" infrastructure. Such devices are marketed as convenient, more energy efficient, and cheaper in the long run, so installing them seems like little more than sensible town management. But most such devices also incorporate – or can be retrofitted with – a wide host of sensors and data collection capabilities such as audio, video, and environmental sensors; advanced data analytics to interpret and act on the data streams; and communication infrastructure, such as WiFi, Bluetooth, or cell capabilities.[9] Once so equipped, they become a critical part of urban surveillance infrastructure. During the George

---

[4] *See e.g.:* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016); FRANK PASQUALE, THE BLACK BOX SOCIETY (2015).

[5] *See e.g.:* VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018); Ed Pilkington, *Digital dystopia: how algorithms punish the poor*, THE GUARDIAN, October 14, 2019, https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor (last visited Jan 14, 2021); Colin Lecher, *A healthcare algorithm started cutting care, and no one knew why*, THE VERGE (2018), https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy (last visited Jan 14, 2021).

[6] SOLON BAROCAS & ANDREW D. SELBST, *Big Data's Disparate Impact* (2016), https://doi.org/10.2139/ssrn.2477899 (last visited Nov 10, 2020).

[7] *See e.g.:* Jeffrey Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women*, REUTERS, October 10, 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G (last visited Jan 14, 2021); Galen Sherwin, *How Facebook Is Giving Sex Discrimination in Employment Ads a New Life*, AMERICAN CIVIL LIBERTIES UNION , https://www.aclu.org/blog/womens-rights/womens-rights-workplace/how-facebook-giving-sex-discrimination-employment-ads-new (last visited Jan 14, 2021).

[8] *See e.g.:* Kate Crawford, *Opinion | Artificial Intelligence's White Guy Problem*, THE NEW YORK TIMES, June 25, 2016, https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html (last visited Nov 10, 2020); Alistair Barr, *Google Mistakenly Tags Black People as 'Gorillas,' Showing Limits of Algorithms*, WSJ (2015), https://blogs.wsj.com/digits/2015/07/01/google-mistakenly-tags-black-people-as-gorillas-showing-limits-of-algorithms/ (last visited Jan 14, 2021).

[9] *See e.g.:* Building a Mass Surveillance Infrastructure Out of Light Bulbs, AMERICAN CIVIL LIBERTIES UNION , https://www.aclu.org/blog/privacy-technology/surveillance-technologies/building-mass-surveillance-infrastructure-out (last visited Jan 15, 2021); Kadhim Shubber, *Tracking devices hidden in London's recycling bins are stalking your smartphone*, WIRED UK, 2013, https://www.wired.co.uk/article/recycling-bins-are-watching-you (last visited Jan 15, 2021).

Floyd protests in San Diego, such "smart city" streetlight infrastructure was utilized to search for and create evidence against Black Lives Matter protesters.[10]

New York City has already adopted comparable technologies: LinkNYC, the public WiFi kiosks run by Alphabet (*Google*) subsidiary Sidewalk Labs, has after years of operation still not disclosed a detailed list of sensors included in the kiosks nor how LinkNYC uses the personal information it collects in its ad-driven business model.[11] And despite littering the streets with thousands of sensors, the project has also failed to deliver on its promise to improve New Yorkers' access to the internet and close the digital divide, as kiosks are primarily located in more affluent neighborhoods[12] and do not offer the speed and reliability of a broadband connection.

Law enforcement has long embraced these urban surveillance technologies in all forms, whether deployed through their own procurement, other governmental and public infrastructure, or privately owned. Across the country, hundreds of police departments have partnered with Amazon to subsidize home installation of the company's Ring surveillance cameras, essentially deputizing the public as to their own front yards.[13] While the NYPD has not entered into such partnerships, the department's Domain Awareness System (DAS) has access to more than 20,000 public and private cameras.[14] Originally created as a counterterrorism tool, the DAS integrates a range of sensors like CCTV, automated license plate readers, ShotSpotter audio sensors, and environmental sensors; previously siloed databases; and a combination of analytics and information technology, including pattern recognition and machine learning.[15] The increase of such analytics and predictive policing systems is particularly worrisome considering the unconstitutional and racially biased stop-and-frisk

---

[10] Jesse Marx, *Smart Streetlights Are Now Exclusively a Tool for Police*, VOICE OF SAN DIEGO (2020), https://www.voiceofsandiego.org/topics/public-safety/smart-streetlights-are-now-exclusively-a-tool-for-police/ (last visited Jan 15, 2021).

[11] Ava Kofman, *Are New York's Free LinkNYC Internet Kiosks Tracking Your Movements?*, THE INTERCEPT (2018), https://theintercept.com/2018/09/08/linknyc-free-wifi-kiosks/ (last visited Jan 15, 2021).

[12] *See LinkNYC*, NYC DOITT, https://www1.nyc.gov/site/doitt/initiatives/linknyc.page (last visited Jan 15, 2021); see also Annie McDonough, *DoITT head Jessica Tisch's hard line against LinkNYC vendor*, CITY & STATE, Mar. 4, 2020, https://www.cityandstateny.com/articles/policy/technology/doitt-headjessica-tischs-hard-line-against-linknyc-vendor.html ("CityBridge has failed to install 537 promised LinkNYC kiosks – many of which were set to be built in outer boroughs, which suffer[] from a dearth of the kiosks, which provide free WiFi, telephone and device charging services. CityBridge has not installed a single kiosk since the fall of 2018[.]").

[13] Drew Harwell, *Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns*, WASHINGTON POST, August 28, 2019, https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/ (last visited Jan 15, 2021).

[14] Since the NYPD does not disclose any details or camera counts, the most recent number stems from the following interview with then Deputy Commissioner of Information Technology at the NYPD: *A Conversation with Jessica Tisch '08*, HARVARD LAW TODAY (2019), https://today.law.harvard.edu/a-conversation-with-jessica-tisch-08/ (last visited Jan 15, 2021).

[15] E. S. Levine et al., *The New York City Police Department's Domain Awareness System*, 47 INFORMS JOURNAL ON APPLIED ANALYTICS 70–84 (2017).

practices; utilizing existing police data to predict and set future patterns of policing will simply create outputs and recommendations reflecting these practices.[16]

In recent years, New York has also seen an uptick in the use of biometric recognition technologies – like face, voice, and gait recognition – by police, in housing, schools, mass transit, and on roads and bridges. Biometric surveillance presents an unprecedented threat to everyone's privacy and civil liberties, enabling the invasive power to track who we are, where we go, and who we meet – for example tracking people at protests, political rallies, or places of worship. In August of last year, the NYPD used facial recognition to identify a Black Lives Matter activist during a protest against police brutality.[17] But these technologies are also notoriously inaccurate and racially biased. Numerous studies have shown that face surveillance technologies are particularly inaccurate for women and people of color.[18] And through litigation, the public has learned of the highly flawed, unscientific, and even unlawful practices that pervade the NYPD's facial recognition program.[19] In addition, many biometric technologies rely on the remote monitoring and collection of personal biological characteristics – without one's consent or knowledge. Unlike a password or credit card number, this information cannot be changed if it's compromised or stolen.

Cities increasingly adopt automated decision systems – software tools or processes that automate, replace, or aid human decision-making – to administer services, allocate resources, and make inferences about individuals, groups, or places. Especially where New Yorker's fundamental rights are at stake – such as in welfare, education, employment, housing, health care, the family regulation (or child welfare) system, or the criminal legal system, these technologies all too often replicate and amplify bias, discrimination, and harm towards populations who have been and continue to be disproportionately impacted by bias and discrimination. The NYCLU and our partners repeatedly sought to offer input and

---

[16] Rashida Richardson et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice,* 94 N.Y.U. L. REV. ONLINE 192 (2019), https://ssrn.com/abstract=3333423.

[17] George Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*, GOTHAMIST (2020), https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment (last visited Jan 13, 2021).

[18] *See e.g.:* Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, 1 IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE 32–41 (2019); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PROCEEDINGS OF MACHINE LEARNING RESEARCH (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (last visited Jan 15, 2021).

[19] Clare Garvie, *Garbage In. Garbage Out. Face Recognition on Flawed Data*, GARBAGE IN. GARBAGE OUT. FACE RECOGNITION ON FLAWED DATA, https://www.flawedfacedata.com (last visited Jan 15, 2021).

recommendations through open letters in January 2018,[20] August 2018,[21] March 2019,[22] a comprehensive Shadow Report in December 2019,[23] and have testified before this Committee in January 2020[24] and in November 2020.[25]

The COVID-19 pandemic has only increased urban surveillance. As the disease began to spread, advertising technology providers were quick to provide mass location tracking data—surreptitiously collected and shared without notice or consent—at various scales and levels of granularity to national, state, and local governments (including NYC).[26] Data broker Experian started tracking and microtargeting people most likely to get hit hardest by COVID-19.[27] Police departments deployed drones with thermal imagery sensors and biometric recognition software such as heart rate, sneezing, coughing, and distance detection.[28] And above all, the crisis has reified and deepened many inequities and laid bare the grave impact of lacking access to technology and broadband internet.

Nearly all these applications undermine New Yorkers' constitutional protections, in particular their rights under the First and Fourth Amendments. When police conduct video surveillance over every inch of the City, it chills free speech, expression, and association. When private companies collect the most sensitive minutiae of our private lives, track our locations in perpetuity, and then, without our informed consent, share that data with the government, it destroys individual privacy. And when the government uses that data to track us, investigate

---

[20] Letter to Mayor de Blasio: Regarding NYC Automated Decision Systems Task Force, NEW YORK CIVIL LIBERTIES UNION (2018), https://www.nyclu.org/en/publications/letter-mayor-de-blasio-regarding-nyc-automated-decision-systems-task-force (last visited Jan 14, 2021).
[21] Open Letter to Automated Decision Systems Task Force, NEW YORK CIVIL LIBERTIES UNION (2018), https://www.nyclu.org/en/publications/open-letter-automated-decision-systems-task-force (last visited Jan 14, 2021).
[22] Letter to the Automated Decision Systems Task Force - March 1, 2019, NEW YORK CIVIL LIBERTIES UNION (2019), https://www.nyclu.org/en/publications/letter-automated-decision-systems-task-force-march-1-2019 (last visited Jan 14, 2021).
[23] *See*: Rashida Richardson, ed., *Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force*, AI NOW INSTITUTE, December 4, 2019, https://ainowinstitute.org/ads-shadowreport-2019.html.
[24] NYC Council Testimony In Relation to Automated Decision Systems Used by Agencies, NEW YORK CIVIL LIBERTIES UNION, Jan 22, 2020, https://www.nyclu.org/sites/default/files/field_documents/20200122-nyclu-testimony-automateddecisionsystems.pdf.
[25] NYC Council Testimony on Oversight and Regulation of Automated Decision Systems, NEW YORK CIVIL LIBERTIES UNION, Nov 13, 2020, https://www.nyclu.org/en/publications/testimony-oversight-and-regulation-automated-decision-systems.
[26] *See*: Recovery Data Partnership, NYC Analytics, https://www1.nyc.gov/site/analytics/initiatives/recovery-data-partnership.page (last visited Jan 17, 2021).
[27] Shoshana Wodinsky, *Experian Is Tracking the People Most Likely to Get Screwed Over by Coronavirus*, GIZMODO , https://gizmodo.com/experian-is-tracking-the-people-most-likely-to-get-scre-1842843363 (last visited Jan 17, 2021).
[28] Chaim Gartenberg, *Connecticut suburb deploys "pandemic drones" to try to enforce social distancing*, THE VERGE (2020), https://www.theverge.com/2020/4/23/21232592/connecticut-suburb-westport-pandemic-drones-draganfly-social-distancing (last visited Jan 17, 2021).

us, accuse us of crimes, and put us in jail based upon the faulty conclusions of a biased algorithm, it makes a mockery of the equal protection of the laws. As long as urban surveillance technology is opaquely procured and operated without the necessary guardrails, we will continue seeing undemocratic decision-making, bias, discrimination, and threats to all our rights.

Principles and Good Practices

We commend the City and the Council for enacting important legislation tackling some of these issues, such as the POST Act, the biometric recognition disclosure requirement for businesses, the ban on cashless stores, the decision not to include vulnerable contactless technology in the municipal ID, and the City's settlement regarding Verizon's failed fiber rollout in low-income areas.

In November 2018, New York City joined the Cities Coalition for Digital Rights and signed its Declaration.[29] It builds on five primary principles: (1) Universal and equal access to the internet, and digital literacy; (2) Privacy, data protection, and security; (3) Transparency, accountability, and non-discrimination of data, content and algorithms; (4) Participatory democracy, diversity, and inclusion; and (5) Open and ethical digital service standards. These set crucial guidelines, yet, unfortunately, the City's actions have fallen far short from these promises and little has been done to implement these principles.

For "smart city" technologies to deliver on their goals and promises, we urge the City to consider and implement these key principles:

- *Ban Discriminatory Technologies*. Enact bans on technologies that show discriminatory impact or threaten people's fundamental rights.

- *Community Inclusion*. Impacted people need to have a seat at the table throughout the project's lifecycle.

- *Restructuring Procurement*. The City's procurement process must be more transparent and include sufficient information and details for public review.

- *Impact and Risk Assessments*. The City should require agencies to conduct publicly accessible Racial and Non-Discrimination Impact Assessments and Environmental Impact Assessments before acquiring new technologies and throughout their lifecycle.

- *Clear, Concise Privacy Protections and Policies*. Meaningful notice must include information about the data collection, purpose, limitations, access, sharing, storage, and deletion. It must be clear and prominent and be written in plain language at a simple reading level.

[29] Declaration of Cities Coalition for Digital Rights, https://citiesfordigitalrights.org/assets/Declaration_Cities_for_Digital_Rights.pdf.

- *Privacy by Design*. The City and any involved party must work during all product stages to build privacy safeguards into "smart city" technologies.
    - *Data Minimization.* Only collect the minimal data needed. Clear limits on initial collection of personal information. Data should not be generated, collected, analyzed, retained, transmitted or aggregated excessively.
    - *Security and Encryption.* Data should be encrypted (in transit and in rest) and communications must be authenticated.
    - *Anonymize* data where possible.
    - *Minimal Retention.* Only keep data for as long as necessary.
    - The default way to give consent must be *Opt-In*, instead of *Opt-Out*. People should be in the position to decide how, when, and why their data is processed and with whom it is shared.
- *Data Ownership* must be with the individual where possible. People must have rights over their personal data, as well as data that is derived, inferred or predicted from their data, actions, and behavior.
- *No Third-Party Access*. Clear limitations on the access, sharing, or selling of data. Information should not be accessible for law enforcement without a warrant. Ban the access by or sharing with federal agencies, including Immigration and Customs Enforcement.
- *Open source and Open Standards*. Avoid proprietary solutions, vendor lock-ins, and long-term dependencies. Adopt initiatives like "Public Money, Public Code," which requires publicly financed software developed for public use to share its source code. Standard, interoperable protocols are in general also more secure and better tested.
- *Auditing and Reviewing Mechanisms*. All systems should be subject to independent, transparent review to ensure – and to assure the public – that such technologies are being used appropriately and treating personal information with the care required.
- *Accountability and Liabilities*. New York City must enable both regulatory oversight, and a private right of action, to remedy any violations of New Yorker's right to control their data.
- *Equitable Access*. Ensure technologies serve people and communities in need, not companies' shareholders.
- *Public Education*. Improve digital literacy and privacy education in order to show New Yorkers how technology, whether used by governments or private companies, impacts their lives.

Conclusion

We thank the Committee for the opportunity to provide testimony and for recognizing the need for oversight and regulation of "smart city" technology. The Council has a crucial role to play in setting guardrails, safeguarding New Yorkers' privacy interests and rights, and ensuring people's voices are heard when it comes to the technologies that shape and impact their lives and environments.