HARVARD Kennedy School
JOHN F. KENNEDY SCHOOL OF GOVERNMENT

Statement of
Rebecca Williams
Technology and Public Purpose Fellow at Harvard Kennedy School Belfer Center for Science and International Affairs

Before the New York City Council
Committee on Technology
Hearing on Smarty City Oversight

January 19, 2021

Introduction

Chairman Holden and Distinguished Members of the Committee, thank you for the opportunity to testify today on smarty city oversight, I regret that I could not make this time virtually. My name is Rebecca Williams and I am a Fellow at the Harvard Kennedy School Belfer Center for Science and International Affairs participating in their Technology and Public Purpose (TAPP) project and I am spending the 2020-21 academic year assessing potential risks smart city technology may pose, assessing current policies and practices, and developing recommendations for the public, governments, and vendors to prevent these harms. Prior to my role as a TAPP Fellow, I used my legal and city planning training in a variety of city management roles tackling energy policy, affordable housing, and code enforcement, and spent 7 years of experience as an advocate, consultant, and civil servant developing various government data and IT policies (including many related to open access). While my research is currently underway, I would love to continue a dialogue with the Committee on Technology on this matter and would be happy to share my findings with the Committee at the completion of my fellowship. It should be noted that my testimony hear today is representative of my views and does not reflect those of the Harvard Kennedy School.

Potential Harms of Smart City Technology

First of all, I would like to applaud the New York City Council on hosting this hearing on the oversight of smart city technologies. There has been an uptick of public outcry related to smart city technology use globally, including but not limited to pushback by local activists[1] and scholars[2] to development of the Sidewalk Labs' flagship "smart city" project in Toronto, objection to the use of the Mobility Data Specification[3] in Los Angeles, and concerns regarding the budding Port Covington TIF[4] in Baltimore, as well as public concerns with New York City's very own LinkNYC project potential Amazon's HQ2[5]. Simultaneously, police departments have been under scrutiny for leveraging "smart city" technology as an extension of their surveillance technologies, such as when smart streetlight footage of protesters was shared with law enforcement in San Diego[6]. While many of these concerns have been reduced to "privacy" I would like to share

[1] https://www.blocksidewalk.ca/
[2] https://some-thoughts.org/
[3] https://ladot.io/wp-content/uploads/2018/12/What-is-MDS-Cities.pdf
[4] https://pc.city/
[5] https://www.forbes.com/sites/victoriapavlova/2018/11/08/in-amazons-competition-for-hq2-was-data-the-ultimate-goal/?sh=12e3d37bd039
[6] https://www.voiceofsandiego.org/topics/government/police-used-smart-streetlight-footage-to-investigate-protesters/

with you some additional harms I have outlined in the blogpost "*What's so Dangerous About Smart Cities Anyway? Perspectives on Public Purpose"* on December 16, 2020[7]:

Lack of Community Input

A first order issue is does the community where "smart city" technology will be deployed want it? To know the answer to this question means ongoing engagement with a community and robust dialogue about types of data collection, how that might contribute to the collective good, and all the trade-offs involved. Given the other possible harms involved (see below), projects should not be pursued at all unless the community is on board for an articulated outcome. Challenges for community input on "smart city" technology include ensuring that approval is informed (perhaps via trusted experts and intermediaries) and identifying the appropriate level of approval (e.g., neighborhood v. city, majority v. unanimous). Examples like Sidewalk Lab's poor public reception (procedurally as well as substantively) to their Master Innovation and Development Plan highlight the need for this dialogue to take place before the procurement process takes place. Cities like Boston and Seattle have attempted to systematize community input on "smart city" tech with a Boston Smart City Playbook[8] (which highlights the need for right-tech versus high-tech approaches to civic problem solving) and Surveillance Impact Report[9] processes (which highlights the need for public comment, working group, and council approval of new surveillance technologies).

Erosion of Privacy and 4th Amendment Protections

While community input is a first order issue to deploying "smart city" technology, the rest of these harms are not delineated in any sequential or ranked order. As technology development moves faster than law, there is a trend of technology expanding possible searches by law enforcement and that expansion being challenged in court as a violation of our Fourth Amendment protection from unreasonable searches and seizures. While an individual's actions or movements in public spaces have historically fallen outside the scope of Fourth Amendment protections, recent case law has inspired some legal scholars, such as Andrew Ferguson, to examine how digital may be considered

[7] https://www.belfercenter.org/publication/whats-so-dangerous-about-smart-cities-anyway
[8] https://monum.github.io/playbook/
[9] https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance-

differently. In "Structural Sensor Surveillance" 106 Iowa L. Rev. 47 (2020)[10] Ferguson considers how automated, continuous, aggregated, long-term acquisition of personal data with "smart city" sensors may trigger Fourth Amendment scrutiny under current Supreme Court doctrine. Separate from Fourth Amendment protections, as a matter of public policy, one may consider other harms that may occur from an erosion of privacy including social detriment and a loss of liberty. How are "smart city" technology contracts construing their privacy policies? Lastly, as "smart city" technology collects more and more data that can be used to re-identify people, the cybersecurity of any information collected becomes an integral aspect of overall privacy protections. A data breach could lead to re-identifying someone and causing threats to their safety and wellbeing or economic loss.

Chilling of 1st Amendment Rights

In the U.S. the first amendment protects the five freedoms of: speech, religion, press, assembly, and the right to petition (protest) the government. The surveillance imposed by "smart city" could have a chilling effect on community members feeling comfortable participating in these protected activities for fear of harassment or retaliation by the state. As more instances of filming protestors are documented (such as in San Diego streetlight cameras, Miami University, Hong Kong) one could reasonably anticipate to be filmed and identified in public space. If public space becomes a place where one fears punishment, how will that affect collective action and political movements?

Discrimination / Oppression

Because "smart city" tech is applied to a given neighborhood, it shares the potential for discrimination rife in urban planning and public safety history and also a new power of extending those inequities to the digital worlds term that many have coined as "digital redlining". Potential harms that flow from disproportionate use or disparate community impact include loss of opportunity, economic loss, and social determinants (dignitary harms, constraints of bias). Cities, such as Baltimore and DC[11], have closed-circuit television (CCTV) installed in in majority nonwhite areas, on average, then in majority white neighborhoods. Detroit has come under scrutiny by local activists for using facial recognition

[10] https://ilr.law.uiowa.edu/print/volume-106/structural-sensor-surveillance/
[11] https://cnsmaryland.org/2020/11/19/police-cameras-disproportionately-surveil-nonwhite-areas-of-dc-and-baltimore-cns-finds/

technology in public housing[12], spurring the introduction of Federal legislation[13] to prohibit "the use of biometric recognition technology in certain federally assisted dwelling units." These biases compound as data collection from strategically placed "smart city" and other surveillance technology increasingly inform policy decisions such as predictive policing. Seattle's surveillance law requires Equity Impact Assessment reporting[14] as part of their surveillance technology review process, but to date the city has articulated an inexpertise in measuring this impact other than examining how it comes up in public comment.

Loss of Accountable Government

Lastly as governments continue to outsource technology services to private vendors the vendors at play take on a quasi-government function[15] without many of the accountability measures built into government functions such as public records access, public auditors, or consequences for elected officials if services do not meet community members expectations. Moreover, if care is not taken with data governance, community members may be further vulnerable to corporate influence via "surveillance capitalism." As "smart city" must be considered as a potential extension of police surveillance and its biases, it must also be considered as a potential extension of corporate surveillance. At what point does a single corporation have "vertical integration" (in terms of personal data) of a whole neighborhood? This corporate influence (via data, and sheer size of these vendors) was central to Sidewalk Toronto criticism, Amazon HQ2 criticism, and Port Covington criticism. For the data aspect, some cities have retained data rights in their contacts (e.g., GovEx's Data Ownership and Usage Terms[16]) or "open standards" (Mobility Data Specification) for access to data collected by the private sector but this raises new questions of what data the vendor be collecting and managing and what data should governments be collecting and managing. Namely, does this collection protect individuals and is the collection fit for its purpose[17]? Ultimately data collected for the purposes of consumer payment is more granular than what is needed for collective city planning and very different from data collected for the purposes of law enforcement. In addition to this fitness for

[12] https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html
[13] https://www.congress.gov/bill/116th-congress/house-bill/4008/text?r=11&s=1
[14] https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/additional-surveillance-reports
[15] https://www.resite.org/stories/bianca-wylie-on-the-critical-design-process-of-democracy-in-smart-cities
[16] https://labs.centerforgov.org/data-governance/data-ownership/
[17] https://journals.sagepub.com/doi/10.1177/016555159502100204

purpose considerations, many alternatives[18] to data governance have emerged as potential approaches to navigating data spaces that must consider individual and collective purposes[19], as well as competing individual, corporate, and public interests. How is data access explicitly or implicitly included in "smart city" vendor business models or contracts? (i.e., Is part of the bargain that the vendor retains data as a good in exchange for the hardware they provide?) Where no or less money is exchanged, how is data access considered in public private partnerships and other test bed scenarios?

I am currently receiving feedback on the above outline of harms and some of feedback that I have heard to date includes additional concerns about reflecting community desires (e.g., who decides what data is collected?), additional concerns around data governance (e.g., concerns of consent to collect information), and additional concerns re: procurements (e.g., privatization of public spaces via this technology, vendor lock-in, perpetuating further surveillance solutions at the expense of other solutions). I would be happy to share with the Committee my final outline of harms and related government assessments when they become available.

Conclusion

In addition to examining policy for the oversight of smart city technology procurement, I call on the Committee to consider policy to prevent the harms outlined above. In considering these harms the Committee may want to examine the Public Oversight of Surveillance Technology (POST) Act to see if it sufficiently covers "smart city" technology and expand that legislation beyond the police department to capture surveillance technologies deployed by other departments. As mentioned at the top of the testimony, it would be my pleasure to continue this dialogue with the Committee and share additional findings from my research.

[18] https://foundation.mozilla.org/en/initiatives/data-futures/data-for-empowerment/#10-data-governance-approaches-explored

[19] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3727562