SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

@ The Urban Justice Center
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 PUBLIC SAFETY

&

COMMITTEE ON TECHNOLOGY

&

COMMITTEE ON FIRE AND EMERGENCY MANAGEMENT

NEW YORK CITY COUNCIL

FOR A HEARING CONCERNING,

OVERSIGHT - NEW YORK CITY'S NEXT GENERATION 9-1-1 SYSTEM

SUBMITTED

November 12, 2019

My name is Albert Fox Cahn, and I serve as Executive Director of the Surveillance Technology Oversight Project ("S.T.O.P.") at the Urban Justice Center. S.T.O.P. advocates and litigates for New Yorker's privacy rights, fighting discriminatory surveillance. I commend Chairs Borelli, Richards, and Holden for today's hearing, and for the opportunity to discuss the privacy implications of Next Generation 9-1-1 systems ("NG911")

I. The Promise and Peril of NG911

For decades, 9-1-1 has provided a vital lifeline. From coast to coast, Americans dial the same three digits for help, replacing the need to memorize individual fire, police and ambulance service numbers. Now in the smartphone and smart device era, we welcome additional forms of connectivity to help the public reach emergency responders

Elements of NG911, have been contemplated for more than 15 years, such as adding SMS texting connectivity. Such functionality makes a great deal of sense, given both the increasing dominance of text-based communication and the range of situations where victims would be able to text, but not call, for help. Unfortunately, NG911 includes numerous other features that pose a clear cost but give an uncertain benefit.

According to the 2018 Annual Report on Implementation of New Generation 9-1-1 in New York City, NG911 will enable the public to transmit digital information to emergency responders, including "data, photos, and video" and integrate with internet of things ("IOT") devices. While there are a limited array of situations where photos and videos may be helpful to the public, there must be safeguards to prevent abuse and NG911's transformation into a mass surveillance tool.

The concerns for NG911 in the criminal justice context are stark. Whether its neighbors in our own apartment buildings, or strangers on the street, NG911 will make it easier than ever to turn each and every smartphone into a government surveillance tool. With a few clicks, video, photos, and location data can be sent to the NG911 system, all without any notice to the person being surveilled.

We fear that NG911's expansion of citizen surveillance will disproportionately impact the Black, Latin/x, Arab, Asian, and immigrant New Yorkers who have long been overpoliced. After all, this is the enduring legacy of stop-and-frisk, and broken windows policing.[1] We must be watchful to ensure that we never again allow the tools of public safety to transform into the mechanism for racial profiling.

The parallels are even more direct when we see the toll taken by public surveillance programs like "See Something, Say Something." These public reporting schemes can give the veneer of governmental legitimacy to plain racial profiling and fearmongering, reports that reveal more about the prejudices of the caller than the behavior of those being reported.

---

[1] Floyd v. the City of New York https://ccrjustice.org/sites/default/files/assets/files/Floyd-Liability-Opinion-8-12-13.pdf. The NYPD made millions of stops throughout the life of program, nearly 90% of which targeted Black and Latino males. District Judge Scheindlin found "the city adopted a policy of indirect racial profiling by targeting racially defined groups for stops based on local crime suspect data"

In a recent Massachusetts case, an entire subway line was delayed for a police investigation when riders merely "noticed two people that appeared to be Middle Eastern."[2] In California, the ACLU has documented numerous individuals who were listed in Suspicious Activity Reports for simply being of "Middle Eastern Descent" or "speaking a foreign language."[3] And just a few weeks ago, a New York City ferry operator kicked Muslim families offboard for being a "security risk"[4]

One can only imagine how many New Yorkers will have their videos and photos submitted through the NG911 system when the same biased public is given this new monitoring tool. The question then becomes what safeguards will be added to ensure NG911 data protects, and doesn't profile, New Yorkers.

II. Unanswered questions about NG911 data retention and use.

During the design and development of the NG911 system, City and private sector stakeholders should actively engage with the public to provide detailed and accessible information on how NG911 will promote and protect New Yorkers' privacy. The following is a list of key questions that remain unanswered at the time this testimony is being prepared, but there are certain to be additional questions as the program goes forward.

Data Retention:

- How long will photos and videos be stored?
- Who will have access to the videos or pictures allegedly documenting "suspicious activity"?
- What safeguards will be in place to prevent disclosure of such videos to the public or press, including, but not limited to, access controls, digital watermarking, and access logs?

Data Sharing:

- Will photos and videos, including those revealing third parties' personally identifying information, be shared with all officers, just responding officers, or some other subset of officers?
- Will such data be shared with other agencies, including via the joint-terrorism task force, High Intensity Drug Trafficking Area program, or other information sharing agreements?
- Will data be shared with other state and local agencies?
- Will Data be shared in real time, or will historical data be available as well?

Augmentation and Coordination:

- Will videos and photos be used by the NYPD's facial identification section as facial recognition probe images?

---

[2] *MBTA: Scare Over Praying Muslims a 'Misunderstanding',* Boston Magazine, https://www.bostonmagazine.com/news/2016/06/17/muslims-praying-t-incident/
[3] *Revision of Suspicious Activity Reporting Functional Standard*, ACLU, https://www.aclunc.org/sites/default/files/asset_upload_file444_12586.pdf
[4] *NYC Ferry Denied 3 Muslim Families Boarding Over 'Security Issue': Complaint*, NBC New York, https://www.nbcnewyork.com/news/local/NYC-Ferry-Denied-Muslim-Families-Boarding-Over-Security-Issue-Complaint-563270222.html

- Will videos and photos be analyzed using any other form of biometric analysis?
- Will data from the NG911 system be integrated into information flows analyzed by either the Domain Awareness System or Real Time Crime Center.

The answers to the forgoing questions are currently unclear, and they will depend on the countless design choices made during the development of NG911. It is essential that the City partner with impacted communities and civil society groups to ensure that the system we create will protect all New Yorkers.

III. Sanctuary City Protections

These queries bring me to my final topic: New York City's commitment to being a sanctuary city. The information collection enabled by NG911 potentially poses a risk to New York City's undocumented and mix-status families. The photos and videos submitted by bystanders could easily be scanned by U.S. Immigration and Customs Enforcement's ("ICE's") facial recognition systems. Within a matter of minutes, a bystander video could become a targeting point for ICE agents.

Unfortunately, New York City's 2017 sanctuary city laws largely exempt the NYPD, leaving them unbound by the privacy guarantees that we hoped would safeguard immigrant New Yorkers. Initiatives 1557-A and 1588-A enacted comprehensive protections against information-sharing with third parties, including the federal government, but then completely carve out information relating to law enforcement investigations.[5] Similarly, these measures would not apply to any data received by the NG911 system in connection with a police investigation.

We must enact the statutory and regulatory protections to ensure that NYPD and other public safety agencies will never permit ICE or federal agencies who share information with ICE to weaponize NG911 against immigrant communities. As we have seen with numerous other bills pending before the council, data collection raises unique safety concerns for immigrant communities. These concerns motivated Introduction 1706-2019, which is currently pending before the Council, and which would prevent City agencies from adding radio frequency tracking chips to New York's IDNYC cards. As with potential aspects of NG911, the danger to our immigrant neighbors simply outweighed any conceivable benefit.

Rather than risk the sort of debate and controversy that has emerged with the IDNYC tracking chip, the agencies developing NG911 can prevent any public pushback before it starts by maintaining open lines of communication and robust avenues of engagement with impacted communities. Similarly, we believe that the Council's ongoing oversight will be essential in ensuring that this new platform helps every single New Yorker feel safer.

Let me be clear, I do not oppose NG911. Rather, I urge the City to integrate the safeguards against abuse, misuse, and mission creep that are needed to ensure NG911 remains a public safety protection and not a perpetual surveillance web. I thank you for giving me the opportunity to address this urgent issue, and I look forward to working with the Council on NG911 deployment.

---

[5] N.Y.C. Admin. Code. § 23-1202(d)(1)(a) "This subdivision shall not require any such notification where the collection or disclosure is by or to the police department in connection with an open investigation of criminal activity;"