

STATEMENT OF RUBEN BELTRAN CHIEF OF INFORMATION TECHNOLOGY NEW YORK CITY POLICE DEPARTMENT

BEFORE THE NEW YORK CITY COUNCIL COMMITTEES ON PUBLIC SAFETY, TECHNOLOGY AND GOVERNMENTAL OPERATIONS COMMITTEE ROOM, 250 BROADWAY, 16th FLOOR NOVEMBER 20, 2023

Good afternoon Chair Hanks, Chair Gutierrez, Chair Ung and members of the Council. I am Ruben Beltran, the Chief of the Information Technology Bureau of the New York City Police Department (NYPD). I am joined today by Scott Semone, Director of the Life-Safety Systems Division, and Juliane Farruggia, the Managing Attorney of the Department's Legislative Affairs Unit, as well as our partners from the Department of Records and Information Services (DORIS), and the Mayor's Office of Media and Entertainment (MOME). On behalf of Police Commissioner Edward Caban, I would like to thank you for this opportunity to discuss the importance of the Department's radio infrastructure to public safety.

It is the NYPD's mission to keep those who live in, work in and visit our city safe, and the number one tool we have in accomplishing that goal is the skill, passion and dedication of the men and women who put on the NYPD uniform each day. To this end, the Department remains committed to providing our officers with the best technological tools to further this objective. Leveraging the latest technology is imperative, and there is no more important single piece of equipment to keeping New Yorkers and officers safe than the simple, everyday police radio. Without this lifeline to Central Dispatch and other officers, the entire concept of how we provide public safety would look very different. The radios our officers carry and the infrastructure that supports them are, quite simply, the backbone of policing in this City, and it has been that way for decades.

Now, I just said that radios are "simple," and they may seem that way to the uninitiated, but that could not be farther from the truth. In our unflinching quest to remain at the cutting-edge of policing and technology, the NYPD is constantly upgrading and adapting our communications systems and what we have now is a fully integrated, modern radio system which works seamlessly both above and below ground in transit and tunnels. This system is currently comprised of over 300 radio antenna sites around the city, as well as hundreds of other forms of transmission sites, to support the 42,000 radios our members carry, as well as the two independent and redundant Public Safety Answering Centers, or PSACs, which field and route 911 calls for service. All of this is necessary to ensure the millions of 911 calls and radio runs our officers respond to every year are relayed seamlessly, saving countless lives. To put this in perspective, last year there were 7.9 million of these radio runs and year-to-date so far we have had 7.2 million. In each of these calls there are many, many more individual radio transmissions between Central Dispatch and uniform police officers in the field. This is without mentioning the millions upon millions of times radios are used in other contexts every year. Our system really shows the extent of its capabilities during large scale events such as New Year's Eve, parades and mass protests where if officers are not able to communicate with Dispatch and each other, things could spiral out of control quickly and many lives would be put in danger.



But more can always be done. As part of the Department's Technology Refresh Project, the Information Technology Bureau is upgrading our radio system with new radios, transmitters, radio Dispatch consoles, antenna systems and associated cables and components. We are moving from conventional analog to the public safety P25 Digital standard, which requires the installation of fiber-optic Ethernet circuits in 300-plus locations throughout the city. By the end of 2024, the entire system will be fully digital, increasing the quality and reliability of every aspect of the radio communications system citywide, and remaining in compliance with FCC guidelines. This project is a massive undertaking and is projected to cost \$390 million by the time it is completed, with approximately \$190 million going to infrastructure and approximately \$200 million to purchase and replace existing portable devices. This is money that has been budgeted for and is absolutely necessary to ensure we stay ahead of the curve in this aspect.

Beginning this summer, the NYPD began the transition to the new system in Brooklyn North precincts, and as of today Brooklyn North is fully upgraded to the P25 Digital system. This also has the effect of fully encrypting the radio communications in these zones. This encryption is necessary to ensure operational safety and security. Criminal groups have been known to monitor the radios in order to strike vulnerable areas when officers are required to respond to events at other locations. Encryption is also necessary to achieve the highest levels authentication, network access control and informational security, as well. The identities and locations of victims and witnesses may be compromised without securing our communications, putting people's safety at risk. It would be irresponsible and a dereliction of our duty not to do everything in our power to prevent this information from getting to people who would harass or harm our vulnerable population.

Importantly, this transition is necessary because unfortunately, the one thing the existing system is not immune to is unauthorized interloper cyber-attacks in the form of electronic warfare on our channels. Off-the-shelf portable radio technology which enables people with malicious intent to access our channels has become far more sophisticated, while at the same time becoming far more accessible and less expensive. In recent years, we have seen numerous incidents where interlopers have used our radio frequencies to disrupt police operations. Examples include fake "officer down" transmissions to draw officers away from a given area, officers' lives being threatened over the air, fake bomb threats, or simply jamming our radio frequencies, temporarily disrupting our ability to respond to legitimate communications. Several years ago there was a concerted online effort to instruct individuals on how to interfere with NYPD radio communications and these threats will only become more commonplace. More broadly, we have no way of knowing who is listening in on our radio transmissions and tracking where our officers are responding. The P25 Digital system will allow us to know exactly who is accessing the system and where they are because a special key is necessary to get into the system. Notably, since these precincts' communications have been encrypted there have been zero instances of interloping on these channels.

Hundreds of police departments and first responder organizations encrypt their radio communications, including federal law enforcement, the Port Authority, major cities such as Chicago, Denver, Washington D.C., New Orleans, St. Louis, Las Vegas, Albuquerque, Nashville, Fort Worth, Houston, San Antonio and Milwaukee, as well as our neighbors in Nassau and Bergen counties. The lack of encryption presents a specific challenge when it comes to federal law



enforcement agencies such as the FBI. New York is a city like no other, and the unique threats our city faces requires unparalleled collaboration between the NYPD and federal law enforcement. But because our current system is unencrypted it does not enable radio interoperability between the federal communications systems and ours. The Department's use of the P25 Digital standard allows authorized roaming and network access between neighboring Land Mobile Radio networks, where secure joint operations can be unified across multiple agencies.

We have heard the concerns over transparency, and some claim that the need for this specific kind of broad exposure outweighs the many downsides and dangers of remaining unnecessarily vulnerable when the technology exists to prevent it. We respectfully, but adamantly, disagree. The NYPD is the most transparent police force in the country and we operate under numerous levels of oversight and accountability measures, and allowing the status quo to continue will unnecessarily put our city at risk and prevent our dedicated officers from using the advanced technology needed to allow them to fulfill their public safety mandate. There are minimal substantive gains in transparency to be made with regards to everyday New Yorkers by remaining unencrypted, which we believe would be insignificant to nonexistent, as there are numerous other avenues for people and elected officials to be kept abreast of the goings-on in their communities. Every police radio communication is recorded and may be made public through Freedom of Information requests. The Department often proactively publicizes radio calls of notable incidents. The Department pro-actively embraced a citizen's right to record our officers from a safe distance, even prior to city and state laws codifying that right. Last year, we began allowing elected officials and other stakeholders access to our operations emails which alert recipients in real time of notable incidents. Each precinct commander works to develop relationships and open lines of communication with community stakeholders and the electeds in their precincts and are often in communication with them in short order regarding incidents affecting their constituents.

What this encryption will not impact, except in a positive way, is our ability to provide public safety. We have always coordinated with other public safety agencies and organizations, such as FDNY/EMS, Homeless Services, Health and Hospitals, the Seagate police department in south Brooklyn, as well as volunteer first responder organizations to facilitate direct access to our radio waves. We have not denied access to any public safety agency or organization who has requested access and encryption will have no impact on our commitment to public safety in all forms.

We have also heard the concerns expressed by the journalism community over encrypting our radios. The NYPD understands the vital importance responsible journalism has to keeping the public aware of safety concerns in their neighborhoods, and the Department provides information to reporters many times a day, every day. We look forward to continuing the dialogue as to how this information landscape will take shape in light of the P25 Digital implementation.

Thank you for the opportunity to speak with you today, and I am pleased to answer your questions.

Testimony of the

New York City Mayor's Office of Media and Entertainment to the New York City Committees on Public Safety, Government Operations and

Technology regarding Media Transparency

Monday, November 20, 2023

Good afternoon, Chairs Gutierrez, Hanks, Ung and members of the New York City Council committees on Technology, Public Safety, and Government Operations. My name is Samer Nasser, and I am the Executive Director of the Press Credentials Office (PCO) with the Mayor's Office of Media and Entertainment (MOME). I am joined today by MOME Senior Counsel Stanislav Skarbo. Thank you for the opportunity to testify on this important conversation on Media Transparency.

Journalism plays a critical role in maintaining a healthy democracy and the Administration unequivocally supports the freedom of the press to do their work. The press provides information that educates, informs and encourages civic engagement. The ability of New Yorkers to express informed opinions depends on their access to objective information about what's happening in their community and beyond.

PCO's mission is to provide members of the press with a timely, transparent, and equitable Press Card application process. Prior to joining MOME, I spent over two decades working as a journalist right here in New York City. At MOME, I leverage my experience in understanding the needs and challenges of newsgathering to serve and fully support Members of the Press to exercise their First Amendment rights. For me, this is both a professional and personal responsibility.

For over a century, the City has been providing qualified journalists with press credentials that allow members of the press to pass police and fire lines, and similar barriers, as well as attend City government press conferences and other events sponsored by the City that are open to the press. To be clear, a press card is not a license, nor is it required to work as a journalist in New York City. It merely allows access to certain areas that would otherwise be restricted to the public for the purpose of newsgathering and informing the public.

Today, this key duty is MOME's responsibility. In 2021, City Council passed Local Law 46 which transferred the function of issuing press credentials from the NYPD to MOME. Local Law 46 also made the following changes: It requires a hearing at the Office of Administrative Trials and Hearings (OATH) prior to suspension or revocation of a press card; it provides a press card applicant with an opportunity to appeal a denial of a press card at OATH; and it requires MOME to offer at least three types of press cards including reserve, standard, and single event press cards. In addition, Local Law 46 required rulemaking.

As of January 20, 2022, the PCO assumed responsibility for issuing press cards. Soon after, MOME issued regulations covering press credentials after a public hearing at which members of the press and First Amendment attorneys provided feedback on the proposed regulations.

The PCO is proud of the service it provides to journalists. Since assuming this key function, we work on ensuring the application process is as smooth as possible and that language barriers and other obstacles have been removed. Our biggest accomplishment is the digitization of the press credentialing application process. The PCO developed an online portal for both application submissions and application assessment. Everything related to press credentialing is centralized on a seamless and user-friendly portal that's accessible from anywhere with internet access. Applicants may apply, appeal, renew and report a press card lost/stolen online at any time.

The PCO website is written in plain language and offers detailed information and video webinars to help journalists navigate the press card application process. To better serve and ensure accessibility for our limited-English proficient constituents, the PCO provides materials in multiple languages. The press credentials portal is available in all 10 citywide languages and journalists may submit media files in any language.

To better assist ethnic and community news outlets in New York City, the PCO works with the Center for Community Media (CCM) at the CUNY Craig Newmark Graduate School of Journalism which offers free workshops to NYC's Ethnic and Community Media Group members.

The PCO has received approximately 3,500 applications and has approved about 70 percent (2,395 press cards), since MOME began assessing applications. Our staff prides itself on being available to guide members of the press on how to obtain a press card in accordance with MOME's rules. Our customer service survey provided excellent feedback. Nighty-two percent of applicants awarded the PCO 4 and 5 star ratings, describing it as, "very well organized. Fast and efficient." Eighty percent of applicants believe the new process is better. These numbers illustrate PCO's commitment to facilitating the critical work that journalists do each day to keep the public informed.

Thank you for the opportunity to testify about the work of the PCO today and we look forward to your questions.

Testimony of Pauline Toole, Commissioner of the Department of Records and Information Services

Before the Governmental Operations, Technology and Public Safety Committees, New York City Council November 20, 2023

Good afternoon. My name is Pauline Toole, and I am the Commissioner of the New York City Department of Records and Information Services, known as DORIS. Thank you, Chairs Ung, Gutierrez and Hanks and the members of the Committees on Governmental Operations, Technology and Public Safety for the opportunity to testify before you today on the proposed local law to add elected officials' social media posts to government social media content maintained by DORIS.

This administration is committed to ensuring that government is open, accessible, and transparent, so that residents of New York City can engage with City government in a meaningful way. Providing access to government records helps accomplish that goal.

Introduction 0961

Intro. 0961 would amend the City Charter to require that DORIS maintain a publicly accessible and searchable online database of the official social media posts and websites of government officials and require the City's elected officials and agencies to provide DORIS with a list of each official social media account annually.

DORIS appreciates the Council's focus on gathering and making available all City government social media posts. We have one suggestion to improve compliance which is to require the account holder and contact information be provided.

The Charter gives DORIS three responsibilities related to the City's records. The Municipal Archives accessions, preserves and makes available City government's historical records, which are the unpublished records of government agencies and officials. The Municipal Library preserves and makes available the published records of City government. The Records Division sets records retention policies and works with agencies to modernize the management of their records—in all formats.

Social media posts and websites are official government records, as defined by the City Charter. In 2017, DORIS published a policy making the retention period for these records permanent and

because they are published, their long-term retention is in the Municipal Library collection, not the Municipal Archives. Recognizing the challenge for agencies to transfer every post to the Municipal Library Collection, DORIS worked with the Law Department and City government's technology leaders to identify and engage a vendor to harvest all official social media posts from government offices. At that time, a separate vendor gathered content from government websites. Both types of records document the business of City government and will be invaluable resources for future researchers.

Currently, there are 28,722,188 posts available in a searchable public database. The site is constantly updated by the vendor, Civic Plus, formerly known as Archive Social. Content is pulled from Twitter (aka X), Facebook, Instagram, Flickr, LinkedIn, Pinterest, Vimeo, YouTube, and, briefly from TicTok. Even though this harvesting began in 2017, the algorithm searches for all posts associated with an account dating to its inception. As a result, some social media posts available on the site date to 2002. For this reason, the requirement that officials provide DORIS with an annual list of accounts suffices because the application will crawl for content created using the various social media platforms.

In our experience, the most challenging aspect of preserving these government records is locating the correct point of contact in an office, which frequently requires some detective work. The list of accounts alone will not allow DORIS to preserve that material. The name of a designated person – who has access to the login credentials – must be provided. It would be extremely helpful to require that the offices and elected officials provide the name and email address of the account holder, the platform name and the name of the account and, if the account holder does not manage social media, the name of the person designated to manage the content.

Finally, we would like to clarify that providing a link to the online database of City government's social media, or its successor, on our agency website meets the intent of this bill which requires that DORIS "Maintain a publicly accessible and searchable online database that contains all publicly viewable content and metadata shared by an official government social media account."

We commend the City Council for its focus on records retention and preservation and would be happy to take any questions you may have.



STATEMENT OF PUBLIC ADVOCATE JUMAANE D. WILLIAMS TO THE NEW YORK CITY COUNCIL COMMITTEES ON PUBLIC SAFETY, GOVERNMENT OPERATIONS AND TECHNOLOGY NOVEMBER 20th, 2023

Good afternoon,

My name is Jumaane D. Williams, and I am the Public Advocate for the City of New York. I would like to thank Chair Gutiérrez, Chair Ung, Chair Hanks, and the Committee members for holding this hearing.

It is important that the New York Police Department is able to conduct ongoing investigations safely and responsibly. As a Council, we must do everything in our power to assist the NYPD so there are no interferences into ongoing investigations. However, we must also balance the need for public safety with the need for transparency. This past summer, the NYPD introduced a \$500 million radio system that encrypts radio communications, a project which will take five years to complete, although several frequencies have already been encrypted. The NYPD has a long history of shirking oversight and accountability, making this move particularly concerning. As of November 20th, 2023, there are 10 precincts using encrypted channels without any accommodations for the press. This hurts the ability for journalists to research criminal cases and conduct a proper journalistic review, which has led to evidence that exonerates formerly incarcerated individuals. The NYPD argues that there will be an accreditation process for journalists at some point. The issue still remains that if police radios are encrypted, then "un-accredited" journalists will need to submit FOIA requests just to hear deciphered transcriptions of the radio. The City of New York already struggles to answer FOIA requests in a timely manner, as some requests take years to process—and the NYPD in particular routinely drags its feet when responding to requests for records and body-worn camera footage, taking months or even years to fulfill requests, if they do so at all.



There are civic reasons to keep the radios available to the public as well. Cab drivers will listen to police radio because they want to avoid active police or EMT events on the road. Additionally, many local crimes are recorded over police radio that do not get media attention, and it is valuable to have a live report about the crime. There are also civilian community patrols that utilize the police radio to help assist the NYPD. There are instances where community patrol groups have stopped active crimes from occuring before the police arrive because of open police radio. Additionally, access to police radio transmissions provides helpful information for protestors, allowing them to avoid police brutality and arbitrary arrests; further, during the 2020 Black Lives Matter protests, individuals monitoring heard officers policing protests make unacceptable comments, including telling each other to "shoot those motherf*ckers" and "run them over."

Furthermore, there may be alternatives to mass encryption. During an active SWAT raid or for certain EMT situations that may lead to a HIPAA violation, some municipalities require that radios are switched to a different communication channel². Furthermore, when there is sensitive coordination between police units, then there might be an option for encrypted channels that can be used, but in most cases a main channel should be used. The NYPD can use the latest technology to protect officers and simultaneously protect the freedom of the press. It cannot be an all or nothing approach. Thank you.

¹ https://citylimits.org/2023/08/25/opinion-city-council-must-act-to-keep-nypd-radio-public/

² https://wiki.radioreference.com/index.php/Encrypted_Agencies#United_States



Protecting the Underserved: Testimony of Andrew Frame, CEO of Citizen, Before the Committees on Public Safety, Technology, and Governmental Operations - New York City Council, November 20, 2023.

Good afternoon.

My name is Andrew Frame. I am the founder and CEO of Citizen, and I am honored to be here to speak about a product and company I started right here in New York City. I came up with the idea for Citizen and built the prototype about a mile away from where I am standing, testifying before you all.

The threat and proposed introduction of radio encryption by the New York Police Department is a crucial turning point for safety in New York city. It threatens to shut down and erase years of extraordinary technological and public safety progress our New York City Citizen team has made, which is working to help keep New York City, and most importantly our most underserved communities safe.

First, some background. I came up with the idea to build a global safety network powered by the everyday citizens of the world, the 6.5b + smart phones they collectively own, and their strong will and desire for their own personal safety as well as their love for their community. My premise was to democratize all real-time crime and fire information and give it directly to the people, the Citizens themselves. For example, when there is a fire in your building, why wouldn't you be notified in real-time at the same time as the fire department? Doesn't it seem obvious to give people more time to get out safely? Another example, when a child is kidnapped, why wouldn't we immediately activate the 10s of thousands of nearby people to be on the lookout? The vision is to make kidnapping nearly impossible. I saw my idea from before we had a single user or even had started developing the product, as timely, necessary and inevitable.

Fast forward to now. Since that day, we have signed up more than 15 million users across our major national cities, we've issued more than 10 billion real-time location-based critical safety notifications, and have helped save countless lives. Our over 15 million Citizen users have received real-time hyper-local safety notifications for over 30,000 Fires, over 28,000 assaults, and over 50,000 events involving weapons. We could not be more proud. It's hard to measure the impact of this transparency, as we don't always hear in the moment how it might have saved a life. But you don't have to search far to find a New Yorker who has a story about how Citizen helped save them or somebody they know.

Our biggest and most important market is the one we started in, New York City. Citizen's impact on New York City has been beyond anything we could have imagined the day it hit Apple's App Store. More than 3.5 million New Yorkers have signed up to Citizen and we have become an essential component of day-to-day life here in New York City. The NYPD clearly sees value in



our service, which might be why they developed their own competitive app to Citizen. It unfortunately didn't gain any traction. Citizen has been developed by proven technologists, we

have raised over \$100m in venture capital to develop Citizen in order to protect every day people and save lives. Citizen should be working in cooperation with the NYPD, not against or in competition.

We've spoken about the stats and statistics, now let's take a moment to discuss the Citizen user base. Most technology companies have as their earliest users technology early adopters and high income earners. Not Citizen. Our strongest communities and densest user concentrations are among the most underserved communities that are hardest hit by crimes and tragedies. When we activate a city, the underserved neighborhoods explode with and get to scale the fastest. In some of these communities we have a 60%+ adoption rate of our product. These are not communities and people who want Citizen, these are communities that need and require Citizen.

Why is that? There are long-standing inequities in public safety which we are helping to address. For example, when a child is kidnapped or goes missing, if the child happens to be from the upper east side, oftentimes the search can quickly become national or international headlines building up global interest in finding the child. When a child is kidnapped or goes missing in an underserved community in Brooklyn, Queens or the Bronx, this almost never happens. Because Citizen was designed as a fully democratized system, with equal access for all, every kidnapping gets the same exact treatment, regardless of zip code or skin color. We often deal with families from underserved communities who plead for but are unable to get amber alerts, or much interest at all in their missing child. We operate a missing persons desk at Citizen which works tirelessly around the clock powered by technology and community to get the children back to their families. Our missing persons and children desk has initiated over 2,000 activations and searches, with a sizable percentage of them being successful. Just last week a young autistic man went missing and was quickly brought to safety by another Citizen user after the geo-targeted real-time missing person notification.

And right when the need for Citizen and our product has never been greater, Citizen's very existence is now at risk. If the NYPD carries forward with their intention of encryption, it will shut down our largest and most important American market, depriving the people of New York from our product and service. This dangerous policy change represents the destruction of our popular public service and platform here in New York, putting New Yorkers, most importantly our underserved New Yorkers directly in harm's way.



While the rationale for encryption is improving safety for officers, a goal we are deeply aligned with, multiple peer-reviewed independent academic studies have proven that Citizen saves lives and is not linked to any harm to the police force or the public. We have developed extensive policies which are followed in order to help keep police officers safe such as never publishing any sort of private tactical coordination which could jeopardize officer safety.

So in order to continue to provide New Yorkers with this vital connective tissue between our communities and public safety agencies, we are advocating for two potential solutions: Adjust the encryption policy so we continue to get open access to critical real-time safety data in NYC, or give Citizen access to the encrypted radio system, which we need in order for us to continue providing our safety product to the 2.4m New Yorkers who use and depend on it 24/7.

Thank you for your consideration, your time, and your service to all of us. I look forward to your questions and to working with you to develop a solution that will continue ensuring and improving the safety of our fellow NYC residents.



21st Floor 1251 Avenue of the Americas New York, NY 10020-1104

Jeremy Chase 212-489-8230 tel 212-489-8340 fax

jeremychase@dwt.com

November 20, 2023

Committee on Public Safety Kamillah Hanks, Chairperson

Committee on Technology Jennifer Gutiérrez, Chairperson

Committee on Governmental Operations Sandra Ung, Chairperson

My name is Jeremy Chase, and I am a Partner in the Media and Entertainment Group at the law firm Davis Wright Tremaine LLP. My firm represents many of the members of the New York News Publishers Association, the New York State Broadcasters Association, and the National Press Photographers Association, and advises them on all manner of newsgathering issues, so I echo and endorse the testimony of Mr. Donovan, Ms. Kennedy, and Mr. Osterreicher heard earlier.

Today, I appear on behalf of WABC and ABC News, two of the largest and most trusted news organizations in the City and the country at large. ABC has profound concerns about the NYPD's encryption of its police dispatch communications. For decades, police dispatch communications have served as a critical source of breaking news around the City. ABC's newsrooms as well as the newsrooms at various news organizations in the City listen to and deploy their resources in response to these communications, and do so for a variety of reasons:

- 1) To inform the public in a timely and accurate manner of criminal activity occurring in the City.
- 2) To communicate critical public safety information to the public at large.
- 3) To provide on the scene reporting to ensure that the NYPD is doing its job in securing crime scenes, serving the public, and performing its duties.

Transparency via contemporaneous access to police dispatch communications is essential to these aims.

While ABC acknowledges that there may be a need to update and/or upgrade the NYPD's communications systems, it must not do so at the expense of an informed citizenry. Justice Louis Brandeis once said that "Sunlight is said to be the best of disinfectants." Encryption of police dispatch communications, without appropriate accommodations for continued and uninterrupted press access, would cast a pall of darkness on the public's understanding of crime and the NYPD's

response thereto. It would be a disservice to the citizens of New York, and would only result in harm to the public at large.

We strongly urge the Council to take measures to ensure that the press maintains contemporaneous access to this vital source of timely public information.

WABC and ABC News look forward to working with the Council, the NYPD, and other stakeholders on this issue of the highest public importance.

Respectfully,

Davis Wright Tremaine LLP

Jeremy Chase

EMERGENCY PHONE: 718 793-7747

Information Phone: 718 793-2055



Forest Hills Volunteer Ambulance Corps, Inc.

P.O. Box 750617 ● Forest Hills, New York 11375-0617 www.fhvac.org

November 16, 2023

Committee on Public Safety;
Jointly with the Committee on Technology and the Committee on Governmental Operations

Good afternoon Members of the City Council,

Let me begin by thanking you for the opportunity to speak at todays important hearing. My name is Aviv Citron, and I am the President and Chief of the Forest Hills Volunteer Ambulance Corps, Inc. (FHVAC). I have been a member of this agency for the past 28 years, beginning my tenure when I was just 13 years old. Instead of enjoying my school breaks or summer vacation with family and friends, I dedicated my life to this agency. Through my years as a youth corps member, I had the ability, at a young age, to learn what responsibility was really about.

The FHVAC was founded in 1971 when a resident of Forest Hills passed away while waiting 2 hours for an ambulance to arrive. This event triggered a group of Forest Hills residents who were concerned by the long response times of NYC municipal ambulances, to organize a volunteer ambulance corps to better serve their community. Successfully serving the Forest Hills community since 1971, the FHVAC applied to expand our operating territory in 1997 to include the community of Rego Park, to which we were awarded this area by the New York State Department of Health. Having responded to thousands of calls since 1997, our agency applied in 2022 to expand our operating territory to other under served areas of Queens. In 2023, after long testimony and proving a necessity, our agency again successfully expanded our response area, to include Richmond Hill & Kew Gardens.

In 2000, at the age of 18, I successfully completed my Emergency Medical Technician Basic (EMT) course at our agency, which allowed me to begin riding the ambulance, and helping the residents, visitors and guests of our communities. We often received emergency calls at our headquarters via our emergency line, however, the majority of calls we responded to were via the NYPD and EMS radios. During those times, we were authorized by our local Police Precincts' Commander, the 112 precinct, the ability to sign out portable radios during our shift.

I am also a 9/11 First Responder and Survivor on behalf of the FHVAC. Unfortunately, due to my rescue efforts on that day, and the days and weeks thereafter, I have life-long health-related illnesses. In addition, it has been documented by the World Trade Center Health Program, that I am the youngest, surviving, First Responder, documented, on this day, nationwide. On this dreadful day, we had in our possession, an NYPD issued portable radio, which may have saved our lives.

The ability to monitor and use an NYPD radio goes far beyond what the normal person understands. This is a tool. This is a life saving tool. Whether it be for our crew, a Police Officer in need, or an

emergency call. Seconds feel like minutes, and minutes feel like hours. According to an article published in the NY Post on September 16, 2023 (https://nypost.com/2023/09/16/nyc-response-times-to-fires-medical-emergencies-soaring/), the average response time for a 911 ambulance in NYC is 10 minutes and 43 seconds. In an emergency, every second counts. Our average response time is 4 minutes and 27 seconds. More than half of what this article states for NYC 911 units. One reason attributed to our short response time, is us having the ability to listen to the NYPD and EMS frequencies. There is no way to tell how many lives were saved by us having this tool on our belt, however, if at least 1 life was saved, it did its job.

While I understand why the NYPD and the Fire Department (including EMS) want to encrypt their radios, in my opinion, it is extremely detrimental. It is detrimental to anyone who needs an ambulance. "Covering our ears" will do a disservice to residents, visitors and guests of the areas we, and other volunteer ambulance corps serve, as well as to the City of New York as a whole.

In closing, the Volunteer Ambulance & Volunteer Fire Departments throughout the City of New York are here to fulfill one mission, and that is the mission of helping people in their time of need. As volunteers we are not paid. We do not receive any compensation whatsoever. We are here out of the goodness of our hearts. Our agencies rely on third party billing and donations from the communities we serve to keep our doors open. By encrypting these agencies radios, and keeping us in the dark, you will slowly, but surely, close every volunteer Ambulance & Fire Department within the City of New York. Again, this will be extremely detrimental long term, and will be a complete disservice to this City.

I thank you again for affording me this time to speak against radio encryption.

BEFORE THE COUNCIL OF THE CITY OF NEW YORK THE COMMITTEE ON PUBLIC SAFETY JOINTLY WITH THE COMMITTEE ON TECHNOLOGY AND THE COMMITTEE ON GOVERNMENTAL OPERATIONS

 $\begin{array}{c} Testimony\ regarding\ Oversight -\\ Media\ Transparency:\ NYPD\ Radio\ Encryption\\ File\ \#\ T2023-4259 \end{array}$

TESTIMONY OF THE NATIONAL PRESS PHOTOGRAPHERS ASSOCIATION

MICKEY H. OSTERREICHER GENERAL COUNSEL

NATIONAL PRESS PHOTOGRAPHERS ASSOCIATION 70 Niagara Street Buffalo, NY 14202 (716) 983-7800 lawyer@nppa.org

November 20, 2023

Introduction

Founded in 1946, the National Press Photographers Association (NPPA) is a 501(c)(6) non-profit professional organization dedicated to the advancement of visual journalism, its creation, editing and distribution in all news media. NPPA encourages visual journalists to reflect the highest standards of quality in their professional performance, in their business practices and in their personal code of ethics. NPPA vigorously promotes freedom of the press in all its forms. Its members include still and television photographers, editors, students, and representatives of businesses that serve the photojournalism industry.

As both staff photographers and freelance visual journalists, members of the National Press Photographers Association (NPPA) gather and report the news for publication by means of print, radio, television, Internet, and other forms of media. The NPPA commends the members of the Council of the City of New York, particularly those of the Committee on Public Safety (Kamillah Hanks, Chairperson), jointly with the Committee on Technology (Jennifer Gutiérrez, Chairperson), and the Committee on Governmental Operations (Sandra Ung, Chairperson) for exercising oversight regarding Media Transparency (file # T2023-4259) where the NYPD has already implemented and intends to further implement encryption of its radio frequencies.

Because the Committee on Public Safety has jurisdiction over, among other things, the New York City's Police Department; and the Committee on Technology has jurisdiction over technology-related issues in New York City, including the Department of Information Technology and Telecommunications (for non-land use related issues), the Mayor's Office of Media and Entertainment (which now is authorized to issue press credentials), and the dissemination of public information through the use of technology; and the Committee on Governmental Operation has jurisdiction over, *inter alia*, municipal governmental structure and organization, including New York City's Commission on Public Information and Communication; we believe it fitting and proper that these

committees oversee and regulate any and all plans to encrypt radio frequencies used by the NYPD as well as those which have already been encrypted.

NPPA submits this Testimony with the goal of ensuring that the First Amendment right of the public to receive information about what their government is doing is upheld for all those who care about transparency and accountability, through continuing and crucial real-time access by the press to radio transmissions involving matters of public concern.

Background

As a visual journalist with over 40 years' experience in both print and broadcast, I cannot overstate the importance of journalists being able to monitor, in real-time, public safety and law enforcement radio transmissions. During my career¹, I was only able to get to fires, accidents, and breaking news stories, in a timely manner and with a better understanding of the situation I was going to cover, by having heard those radio calls. In one such case, a man who had just shot and killed his wife confessed to me through the open back window of a police car as he was being driven away. That video, properly subpoenaed by the district attorney, led to his indictment and conviction for murder.

As NPPA's general counsel, I have been dealing with the issue of radio encryption on a nationwide basis for well over a year. In New York City, NPPA is part of a New York Media Consortium.

Members of that group met with then NYPD Deputy Commissioner for Public Information (DCPI), Julian Phillips, at One Police Plaza on January 12, 2023, to express our concerns regarding the encryption of NYPD radio frequencies and request real-time unencrypted/de-encrypted access to those transmissions. During that meeting we were assured that no NYPD frequencies had yet been encrypted and that NYPD was just in the "testing" phase. We were asked by the NYPD to "brief" our 'major

3

¹ See Appendix A containing 1979 photo of me on assignment in my scanner-laden car.

concerns and possible solutions regarding NYPD's encryption plans" and on February 20, 2023, we submitted a six (6) page memorandum (See appendix B) addressing this request. The Consortium also had a short Zoom call with the NYPD on June 9, 2023. Despite follow-up calls, emails and a letter, we never received a meaningful response from the NYPD regarding this matter.

In May, Julian Phillips retired. In July, radio transmissions for six (6) Brooklyn police precincts went off-the air as the encryption process was initiated. At that time NPPA issued a statement expressing extreme disappointment that the encryption occurred in Brooklyn despite assurances from NYPD executives that it "would not be happening for some time." This was after we met with them in good faith to express our concerns over how encryption will negatively impact the ability to cover matters of public concern in a time critical manner, which will ultimately impact the public's First Amendment right to be informed. To date NYPD has encrypted at least ten (10) precincts.

On November 2, 2023, New York City Comptroller, Brad Lander, sent a letter to NYPD Commissioner, Edward A. Caban, requesting information regarding the implementation of NYPD's radio encryption. To our knowledge, the NYPD has yet to respond to the comptroller's inquiry, but did issue a statement, that "the safety of our first responders and the community will always remain the NYPD's top priority. The Department works day-in and day-out to be transparent and build trust with the public. We are continuing to explore whether certain media access can be facilitated, including utilizing methods that are already being used in jurisdictions with encrypted radios," (emphasis added). Unfortunately, we are still at a loss to know what that means.

In order to better address this growing concern, on November 17, 2023, NYS Senate Deputy Leader, Michael Gianaris, introduced <u>S07759</u>, a bill enacting the "keep police radio public act," and providing, *inter alia*, "that all law enforcement agencies in the state using encryption in radio communications shall adopt a written radio encryption policy;" and ensuring such policy shall provide

that, that all radio communications, with the exception of sensitive information, are accessible, in real time, to duly authorized media representatives or organizations and to emergency services organizations," (emphasis added). Additionally, "[i]n the event that a law enforcement agency does encrypt radio communications pursuant to this subdivision, the department of state shall, for the purpose of verifying credentials, establish and administer a process for granting real-time access to radio communications to duly authorized media representatives or organizations," (emphasis added.

Analysis/Recommendations

Since 1936, when the NYPD <u>first used "a special short-wave field station</u> to [communicate with] police radio cars and motorcycles" escorting President Franklin D. Roosevelt's motorcade during the opening of the Triborough Bridge, being able to receive police, fire and public safety radio transmissions has allowed journalists to know when, where, and how matters of public concern were occurring, so as to be able to better report them to the public. Countless stories would have gone untold and unseen if not for the ability to monitor these important transmissions using radio scanners, which are only able to receive, but not transmit on these radio frequencies.

Despite our efforts to work cooperatively, other than platitudes, the NYPD has not been forthcoming in any meaningful way or been willing to share its encryption plans, or to articulate its intentions to provide journalists with access to such crucial communication and information in real-time.

As the U.S. Department of Justice (DOJ) noted in its *Community Relations Services Toolkit for Policing* regarding the "Importance of Police-Community Relationships and Resources for Further Reading,"[t]ransparency is essential to positive police-community relationships. When a critical incident occurs, agencies should try to release as much information about it as possible, as soon as possible, so the community will not feel that information is being purposefully withheld from them," (emphasis added).

Additionally, we believe it is instructive that, with regard to encryption of its transmissions, the

NYPD be mindful of the DOJ's *Policing 101* that "[c]ommunity policing is a policing philosophy based on three core components: community partnerships, organizational transformation, and problem-solving." As such, "Community Partnerships" should be collaborative "between the law enforcement agency and the individuals and organizations they serve to develop solutions to problems and increase trust in police," (emphasis added). The DOJ also notes that "Organizational Transformation," is one where "[t]he alignment of organizational management, structure, personnel, and <u>information systems to support community partnerships and proactive problem solving</u>," (emphasis added). And finally, "Problem-Solving" is "[t]he <u>process of engaging in the proactive and systematic examination of identified problems to develop and evaluate effective responses," (emphasis added).</u>

It should be remembered that as communities, visual journalists and the NYPD have far more in common than it first appears. While police "Protect & Serve" journalists "Inform & Serve." Those in both professions rush toward critical incidents while others run in the opposite direction. Neither group can "work from home" and both are often attacked/criticized for doing their jobs. With that in mind, recognizing that community support is a critical factor in the ability of the NYPD and the press to effectively perform their societal functions. The critical but often tenuous relationship between police, journalists and the communities they serve determines whether either group will have community support.

So it is incumbent upon the NYPD to help promote transparency and accountability by allowing journalists' continued access to radio transmissions to foster greater public trust.

Conclusion

As noted in the attached New York Media Consortium Brief, NPPA urges the NYPD (and if necessary, this Council) to develop mutually agreeable protocols for the use of this technology to allow qualified journalists (as defined under Sec. 79-h of New York State Civil Rights Law) access to real-time NYPD communications. We also believe that the language in Senate bill S07759 may be helpful (if not

controlling) in crafting a Council bill.

The NPPA appreciates the opportunity to submit this testimony and looks forward to cooperatively working with these committees along with the NYPD to overcome the challenges facing New Yorkers regarding police radio encryption and to further build public trust through improved transparency and ensured accountability.

Thank you for your attention to this critical issue.

Respectfully submitted,

NATIONAL PRESS PHOTOGRAPHERS ASSOCIATION

By Mickey H. Osterreicher

Mickey H. Osterreicher, General Counsel

70 Niagara Street Buffalo, NY 14202 (716) 983-7800 lawyer@nppa.org

Appendix A



Appendix B



February 20, 2023

Julian Phillips
Deputy Commissioner
New York Police Department
One Police Plaza
New York, NY

Dear Commissioner Phillips:

On behalf of the undersigned organizations, we want to thank you for meeting with us to discuss NYPD's plans to encrypt all police communications. We found the meeting with you and your team most productive and look forward to continuing our discussion. During the meeting you asked us to "brief" our major concerns and possible solutions regarding NYPD's encryption plans. The following memorandum addresses this request.

1. Background – The Need for Cooperation

For years qualified journalists have been able to access NYPD communication. This has allowed qualified journalists to fulfill their fundamental, Constitutional mission to inform the citizens of New York City. Providing such information is essential for a functioning democracy. It also facilitates public safety, by immediately informing New Yorkers of dangerous situations that are occurring throughout the five Boroughs.

We recognize that policing, especially in a city as large as New York City, is inherently dangerous. We salute members of NYPD, who put their lives on the line to keep our city safe. In this regard, we understand NYPD's desire to develop a secure communications system that reduces the risk of harm to members of the service .

While these objectives have sometimes conflicted, we both confront a common issue in today's video world. Regardless of the location or time of day, people with cameras in wireless devices are recording NYPD activities and distributing those videos over social media platforms. Thousands of citizens may

instantly see these recordings and believe them to be accurate. Unfortunately, in many instances these videos may not provide an accurate depiction of matters of public concern. Misinformation from such recordings may make a volatile situation worse, forcing more resources to be expended to ensure public safety. Qualified journalists confront the same issue. Their fundamental obligation to the citizens of New York is to report the news accurately. If qualified journalists are not present at situations involving NYPD activity, and a mischaracterization of those events gains traction on social media, both NYPD and journalists are placed on the defensive after missing the news cycle. Journalists must then expend enormous efforts to retell the story accurately to a confused and perhaps agitated public.

NYPD and qualified journalists both require the public's trust to be effective. By working together, we can avoid the potential harms associated with the distribution of misinformation through the Internet and on social media platforms.

To achieve this objective, we must cooperate so that qualified journalists are able to accurately cover NYPD's activities. This requires access to police communications in <u>real time</u>. Encryption of <u>all</u> NYPD communications undermines this objective. Fortunately, other law enforcement departments that have addressed this issue have been able to strike an appropriate balance between protecting police communications and allowing qualified journalists timely access. We believe these examples can serve as a template for NYPD as it moves forward with its encryption plans.

2. Develop a Mutually Agreeable Protocol and Technology Allowing Qualified Journalists Access to Real Time NYPD Communications

Encryption advocates note that security is necessary to protect the safety of officers in the performance of their duties. They claim that absent some form of encryption, criminals will have access to sensitive information that could place the lives of officers at risk. In addition, they note there may be privacy concerns with allowing journalists access to certain types of information. These concerns can be addressed by developing an encryption system that ensures officer safety, protects privacy and allows qualified journalists access to certain real time information necessary for them to fulfill their mission.

A number of law enforcement agencies have enacted such systems. For example, the California Highway Patrol (CHP) decided not to encrypt its radio communications. Unencrypted CHP transmission only includes basic information. For privacy reasons, personal information, such as criminal history, is carefully guarded and provided via computers. In San Francisco, SFPD will use certain public channels to send officers to an incident, such as asking units to respond to a specific location for a report of a robbery. Other information is protected. At the conclusion of the incident, dispatchers will state on an unencrypted channel what the outcome was, for example, officers took a report or made an arrest.

Recently, the Palo Alto Police department, which had encrypted all its communications, revised its policy to allow access while protecting specific information.

This change provides the public with open access to police radio communications and enhances officer options in securing personal identifying information. The new procedures increase field personnel flexibility by providing three different options they can use to safeguard personal identifying information depending on the situation with which they are presented. Those options are a radio check that transmits only a person's driver license number, a radio check that splits

individual components of personal identifying information into separate transmissions, or a cell phone call to our 24-hour dispatch center.¹

Law enforcement agencies in Las Vegas, Nevada; Pueblo, Colorado and Decatur Illinois have reached agreements allowing credentialed media to access police communications. We believe these jurisdictions can serve as a template for New York City.

Some jurisdictions, such as Chicago, employ a 30-minute delay in providing access to information. Such a delay effectively denies qualified journalists the ability to cover live on the scene events. We believe such a policy is fatally flawed. If a dangerous situation occurs, citizens must be informed by trusted media outlets in real time. As noted above, a delay allows those with wireless devices to record the activity live and transmit possible misinformation of the event throughout the city. Delayed access to information runs counter to the objectives of the NYPD, qualified journalists and most importantly harms the citizens of New York.

We recognize there is additional "tactical" information provided over police communications during hostage situations, active shootings, riots, drug enforcement, gang activity, Emergency Service Unit (ESU) deployment and other events. In these contexts, the safety of law enforcement officers becomes critically important, and access to communications by criminal elements poses a significant problem.

Fundamentally, qualified journalists seek to maintain access to <u>real-time</u> police dispatch radio communications. This information is essential for the coverage of events throughout the city. Access to "tactical" information is worthy of additional discussion, bearing in mind the twin objectives of informing the public and protecting the safety of officers.

Importantly, our proposal would not allow criminal elements to access any such information and place officers' safety at risk. Our approach limits access to qualified journalists that have been recognized under New York Law.

3. Defining Qualified Journalists for the Purposes of Access to Police Communications

During our meeting, a question arose regarding who should be allowed to access NYPD communications. While recognizing a broader right of the public to be aware of police activities, we are proposing a narrower access policy. Under our proposal, <u>only qualified journalists would be allowed access to the relevant police information described above</u>. It is important to find an appropriate definition of "qualified journalist." Fortunately, New York law already has workable definitions.

Other states, such as California, have addressed this issue. In defining the persons eligible to qualify for media access, CA Penal Code §409.7 defines a qualified journalist as "A duly authorized representative of any news service, online news service, newspaper, or radio or television stations or network." New York City and New York State have also addressed this issue.

One approach would be to use the criteria that are currently used in granting press credentials in New York City. While NYPD issued these credentials in the past, press credentials are now issued through the Mayor's Office of Media and Entertainment (MOME) pursuant to Title 43 of the Rules of the City of New

¹ Press Release, Palo Alto Police Department, August 4, 2022 https://local.nixle.com/alert/9580626/?sub_id=0

York Chapter 16.² The criteria employed for issuing a standard press card for an individual or a reserve press card for a newsgathering organization would be appropriate for defining those journalists who would be eligible to access unencrypted police communications.

Another option would be to enact a standard consistent with New York State laws governing the sale of body armor. Under the New York gun law enacted last year, citizens are prohibited from the purchase, possession or sale of body armor.³ The law, however, recognized exemptions for certain professions whose jobs place them at risk. In January, the New York Department of State granted journalists and newscasters the ability to obtain body armor in New York.

The information set forth above supports a determination by the Department that the activities of the professions of "qualified journalist" and "newscaster" sometimes require members of such professions to put themselves in dangerous situations that may expose them to serious physical injury, and that such serious physical injury may be prevented or mitigated by the wearing of body armor. Based on the foregoing and the requirements of Executive Law §144-a and 19 NYCRR Part 905, the Department has designated the professions of "qualified journalist" and "newscaster," each as defined in section 79-h of the New York State Civil Rights Law, as eligible professions and adds such professions to the Department's list of eligible professions.⁴

This definition is relevant to the present situation. For public safety reasons, the New York Department of State wanted to limit the ability of the general public to purchase body armor. As a result, it was very restrictive in defining those professions, including journalists and newscasters, that would be eligible to purchase body armor.

Also, NYPD will have experience applying the new body armor standard. Under the New York gun law decisions regarding who can purchase body armor, including the scope of the journalist exemption, are to be enforced by local police departments. As a result, the definition contained in the body armor exemption for journalists will not be an alien concept. To the contrary, NYPD will have to apply this standard every day. Simply stated, if a journalist is qualified to purchase body armor, they should also be qualified to access unencrypted police communications.

Finally, this plan provides access that is limited to only to qualified journalists. It denies access to those who want to break the law or threaten the police. Under the current system of "unencrypted" NYPD communications, there are virtually no instances where a qualified journalist provided criminal elements with information obtained from police communications. Limiting access to <u>qualified</u> journalists significantly reduces the risks of sensitive information falling into the wrong hands and endangering the safety of members of the service.

² See: https://www1.nyc.gov/assets/mome/pdf/Final Press Credential Rule 2021.pdf

³ See: https://dos.ny.gov/body-armor

⁴New York Department of State, Determination In the matter of requests that "journalist," "broadcast journalist," and "news crews" be designated as eligible professions for the purchase, sale, and use of body armor. January 13, 2023, https://dos.ny.gov/system/files/documents/2023/01/determination-journalist-et-alia.pdf

4. Technical issues: There Will Be no Interference to NYPD Communications.

Encryption advocates argue that it is necessary to prevent individuals from hijacking or otherwise causing interference to police communications. While we do not know the technical specifications of NYPD's proposed system, we can guarantee there will be <u>no</u> interference from our proposal.

To the extent NYPD is developing a new system that is transmitting encrypted information on public safety radio frequencies "over-the-air," it will be placing numerous transmitters and repeaters at various locations throughout the city. As a technical matter, the only way there can be interference is by illegally operating and unauthorized transmitter on the same or an adjacent frequency.

But we are not suggesting that journalists have access to transmitting equipment or transceivers. We are asking to access NYPD communication by using only <u>receivers</u> that can access NYPD transmissions. Like the radio in your car, the receivers used to access NYPD communications are unable to transmit, making it impossible to cause interference with police communications.

There have been instances where police communications systems have received interference from illegal transmitters operating on public safety frequencies. Those instances do <u>not</u> involve qualified journalists who have been listening to unencrypted communications on scanning receivers for years. Those instances involve the illegal use of a <u>transmitter</u> (not a receiver) operating on police frequencies. Such illegal transmissions violate both Federal and New York State laws.

Access to information by qualified journalists may depend in part on the technical architecture of the NYPD's proposed system. For example, New York City covers a large geographic area with precincts throughout the five boroughs. It is likely that a new NYPD communications system will employ a series of transmitters that allows NYPD to cover the entire city, but independently transmit different information in each area. Depending on the geographic coverage area of each transmitter, this could require news organizations to purchase multiple receivers and place them in different locations throughout the city. Purchasing multiple radio receivers that decode encrypted communications could be cost prohibitive.

A low cost approach would be to take <u>real-time</u> NYPD communications and place them on a secure internet service such as *Broadcastify*. https://www.broadcastify.com/ Numerous police and fire departments across the country have already placed their communications on this system. Such a service would allow journalists access to NYPD communications throughout the city using the online service without having to purchase multiple receivers and place them in different locations. With an online service, NYPD could control who is able to monitor such communications by providing individually identifiable access codes.

We understand NYPD is in the process of testing its new system. At this point it is difficult to gauge the technical issues without additional information. Depending on the system's technical architecture, some of our concerns may not arise. We would like to engage in further discussions with NYPD, because the technical aspects of the system can negatively affect access by journalists.

5. Enforcement

We recognize that NYPD has concerns regarding the security of its system. There are two issues. First, how to ensure that only qualified journalists can access the information. Second, what happens if a qualified journalist misuses or allows others to access NYPD encrypted communications.

As to the first concern, we would be happy to discuss implementing data security measures. This would include access to hardware (radio receivers) or digital communications. This could include required key cards to access radio receivers in newsrooms. It could also include requiring authentication to access digital communications. Similarly, we would establish training, best practices and/or a code of conduct to help prevent improper access.

The second concern is based on trust. For years qualified journalists have worked with NYPD in a qualified and responsible manner. When given confidential information from law enforcement, we honor that commitment. The same is true for protecting confidential sources. Journalists who fail to live up to these commitments do not remain in the profession for very long. There is every reason to believe that qualified journalists will not misuse their ability to access NYPD communications. A breach of that trust will make it difficult if not impossible for a journalist to work with NYPD. Indeed, violating this trust could result in disciplinary action by their news organization.

Nonetheless, we recognize NYPD is concerned that communications received by journalists may be misused or used by non-journalists. To this end it is worth discussing administrative mechanisms that may be used by NYPD to ensure compliance. For example, depending on the technical aspects of the system being developed, it may be possible to change transmitting codes and encrypt all radio receivers used by an offending party. If NYPD uses an internet-based system, then it could deny future access by changing access codes. We are willing to discuss a range of options to address NYPD's security concerns.

6. Summary

We appreciate the opportunity to present our views regarding NYPD's proposed plans to encrypt its communications system. We hope this memorandum explains the challenges and opportunities in resolving this issue and can serve as a basis for future discussions. There is a concern that decisions may have already been made regarding the system that is in the process of being tested. We are not sure if the technical aspects of system will limit the potential options for journalists to access these communications. Accordingly, we look forward to continuing our discussion with you in a timely manner. Thank you for your consideration and we look forward to working with you and your team.

Respectfully submitted,

Bruce Cotler, President, New York Press Photographers Association
David Donovan, President, NYS Broadcasters Association
Jane Tillman Irving, past-President, New York Press Club
Diane Kennedy, President, NY News Publishers Association
Thomas Maddrey, Chief Legal Officer, American Society of Media Photographers
Todd Maisel, Government Relations Chairman, New York Press Photographers Association
Lloyd Mitchell, Govt. Relations Committee, New York Press Photographers Association
Mickey H. Osterreicher, General Counsel, National Press Photographers Association
Dan Shelley, President and Chief Executive Officer, Radio Television Digital News Association
Peter Szekely, President, The Deadline Club/NYC chapter, Society of Professional Journalists



Legislative Affairs 125 Broad 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 Committees on
Public Safety, on Technology, and on Governmental Operations
Regarding the Oversight of NYPD Radio Encryption

November 20, 2023

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony regarding the oversight of NYPD radio encryption. 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.

This summer, the NYPD began to encrypt its radio communications, effectively shutting out journalists and members of the public from access to emergency communications. Already ten precincts have adopted encrypted radio technology, with plans for all other precincts to go dark by the end of 2024.1

For almost a century, the press and the public at large have been able to access emergency communications, such as broadcasts on natural disasters, police activity, and other newsworthy information. Although radio technology has changed over the decades, radio scanners continue to provide independent access for journalists and the public alike to receive and respond to breaking news in their neighborhoods. It has also been a crucial tool for police transparency by informing reporters in real-time of the killing of Eric Garner during his arrest in Staten Island, the police shooting of Amadou Diallo, and the police shooting of Sean Bell.² Access to radio communications have also been key for public and press scrutiny of police

-

¹ Todd Maisel, Over and out? City Council Hearing Eyes NYPD Radio Encryption Plan That Could Shut Press and Public out of Breaking Crime News, AMNY (2023), https://www.amny.com/news/city-council-nypd-radio-encryption-hearing-planned/.

² Ibid.

responses at protests against police brutality.³ Public access to emergency communications is a public safety and a police oversight issue. Secrecy undermines trust in law enforcement, it impedes accountability, and ultimately makes New Yorkers less safe.

It bears reminding of the NYPD's substantial history of evading disclosure requirements to avoid public scrutiny. This step towards locking the public out from access to radio communications falls within a broader pattern of secrecy, routinely denying or delaying requests for public records and attempting to shield itself from oversight. This year alone, the NYCLU filed three lawsuits against the NYPD for withholding or delaying the release of vehicle stops data.⁴ Similarly, the effort for the release of officer misconduct data and the repeal of Section 50-a was met with heavy pushback from the NYPD and even more secrecy.⁵

The NYPD has also consistently fought any disclosures of its vast arsenal of surveillance technologies. The Council passed the Public Oversight of Surveillance Technology ("POST") Act in response to the NYPD's long and troubling history of engaging in surveillance tactics that target political dissent, criminalize communities of color, and jeopardize all New Yorkers' privacy. The subsequent disclosures were a clear attempt at releasing an absolute minimum of information.⁶

This latest move to shut out public access to communications that have been readily accessible for decades merits close scrutiny by and skepticism from this body. The NYPD's purported concerns about public safety with respect to their radio communications must be viewed within the context of an agency that has repeatedly and hyperbolically invoked fears about public safety as a means of shutting down debate and erecting a wall of secrecy around its operations. And these concerns must also be weighed against the strong public and journalistic interest in having the ability to monitor and engage in real-time oversight as an independent check against an agency that has historically resisted calls for basic transparency and accountability.

In conclusion, we thank the Committees for the opportunity to provide testimony. Police transparency is a central requirement to ensure public safety and trust. We urge the Council to protect long-standing transparency practices in emergency communications, particularly at a moment when New Yorkers are rightly demanding greater oversight of law enforcement.

³ Joseph Cox, Thousands of People Are Monitoring Police Scanners During the George Floyd Protests, VICE (Jun. 1, 2020), https://www.vice.com/en/article/pkybn8/police-radio-scanner-apps-george-floyd-protests.

⁴ For Third Time This Year, NYCLU Sues NYPD for Traffic Stop Data, NYCLU, October 31, 2023, https://www.nyclu.org/en/press-releases/third-time-year-nyclu-sues-nypd-traffic-stop-data.

⁵ See, e.g., Testimony In Support of S.3695, Repealing Civil Rights Law Section 50-a, NYCLU, October 17, 2019,

https://www.nyclu.org/sites/default/files/field_documents/final_testimony_for_senate_codes_50a_hearing __2019.10.17.pdf.

⁶ Comments on Draft Surveillance Impact and Use Policies, NYCLU, February 24, 2021, https://www.nyclu.org/sites/default/files/field_documents/nyclu_letter_on_post_act_draft_policies_0.pdf.



New York State Broadcasters Association, Inc.

Amended Testimony David Donovan President and Executive Director New York State Broadcasters Association, Inc Regarding NYPD Encryption

On behalf of radio and television stations serving New York City, I want to thank the New York City Council for conducting an important hearing regarding plans to encrypt communications by the New York City Police Department (NYPD). The following supplements testimony submitted previously by the New York State Broadcasters Association, Inc.

During the hearing, reference was made to a memo submitted by media organizations to the NYPD regarding our concerns with its plan to encrypt all communications. As requested by the City Council, I have attached a copy of that memorandum, dated February 20, 2023.

As the memo demonstrates, we have been seeking to work cooperatively with NYPD to address these issues for quite some time. Our objective was to try to resolve issues regarding media access <u>before</u> the deployment of new encrypted radios. Despite numerous attempts at outreach, including a brief virtual call on June 9, 2023, restating our concerns, there has been no meaningful response by NYPD.

NYPD continues to state that it is examining the issue, looking at other jurisdictions and that no decision regarding access by journalists has been made. Based on NYPDs testimony, it appears these issues will not be addressed until encrypted radios are deployed throughout the entire city. Moreover, it would appear the policy decision has already been made. To be sure, NYPD made the decision to deny reporters access and limit citizens' ability to see live on the scene reports from independent journalists in 10 Brooklyn precincts. Given NYPD's testimony, there is every reason to believe NYPD will not permit media access in a timely manner.

During the hearing NYPD referenced cities that have deployed encrypted radios and denied access to the media in a timely manner. NYPD's testimony did not include the example of Las Vegas. Las Vegas deployed encrypted radios but allowed media access. This system has worked well for both the police and the media. As was noted during the hearing, New York City is the media capital of the world. Denying access to the media can affect the information flow not only to the citizens of New York but the nation and the world.

Policy decisions regarding media access must be made <u>before</u> the deployment of new technology. The City Council should not permit NYPD to continue delaying its decision regarding media access until <u>after</u> the encrypted system is fully deployed. To do so means the City Council will be presented with a *fait accompli*, and citizens across New York City will be relegated to obtaining information about police activities from untrustworthy social media sources.

If NYPD truly wants to examine this issue, then it should simultaneously provide a system of media access in those areas where it is deploying new encrypted radios. This would allow both NYPD

and the media to explore which system will work best to inform citizens of events in real time, while also protecting law enforcement. We are more than willing to provide communications engineers to work cooperatively with NYPD to help resolve any technical issues.

As noted during the hearing, we salute NYPD for its tremendous work in keeping the citizens of New York City safe. Every day, law enforcement officers put their lives on the line. Their safety should be a priority. However, journalists are not the problem. NYPD provided no evidence demonstrating that allowing communications access to journalists endangers the lives of its officers. Individuals using illegal transmitters to interfere with police communications are breaking both state and federal law. Criminals scanning police communications to aid in their illegal activity should not have access to police communications. But that is not us. The City Council and NYPD should not conflate the need to prevent these activities with access to basic dispatch information by qualified professional journalists. To this end, the policies regarding body armor adopted by the New York Secretary of State can serve as a model for allowing access to professional journalists.

The testimony presented at the hearing demonstrates that the New York City Council should act <u>now</u> to address the issue of media access to NYPD encrypted communications. Unfortunately, it appears NYPD wants to "study" the issue until it is too late for the City Council to act. We hope this will not be the case. We look forward to working with the City Council and NYPD to address these important matters.

Respectfully submitted,

David L. Donovan

President

New York State Broadcasters Association, Inc.

1805 Western Avenue Albany, NY 12203

(518) 456-8888

ddonovan@nysbroadcasters.org

Date: November 23, 2023



February 20, 2023

Julian Phillips
Deputy Commissioner
New York Police Department
One Police Plaza
New York, NY

Dear Commissioner Phillips:

On behalf of the undersigned organizations, we want to thank you for meeting with us to discuss NYPD's plans to encrypt all police communications. We found the meeting with you and your team most productive and look forward to continuing our discussion. During the meeting you asked us to "brief" our major concerns and possible solutions regarding NYPD's encryption plans. The following memorandum addresses this request.

1. Background - The Need for Cooperation

For years qualified journalists have been able to access NYPD communication. This has allowed qualified journalists to fulfill their fundamental, Constitutional mission to inform the citizens of New York City. Providing such information is essential for a functioning democracy. It also facilitates public safety, by immediately informing New Yorkers of dangerous situations that are occurring throughout the five Boroughs.

We recognize that policing, especially in a city as large as New York City, is inherently dangerous. We salute members of NYPD, who put their lives on the line to keep our city safe. In this regard, we understand NYPD's desire to develop a secure communications system that reduces the risk of harm to members of the service.

While these objectives have sometimes conflicted, we both confront a common issue in today's video world. Regardless of the location or time of day, people with cameras in wireless devices are recording NYPD activities and distributing those videos over social media platforms. Thousands of citizens may

instantly see these recordings and believe them to be accurate. Unfortunately, in many instances these videos may not provide an accurate depiction of matters of public concern. Misinformation from such recordings may make a volatile situation worse, forcing more resources to be expended to ensure public safety. Qualified journalists confront the same issue. Their fundamental obligation to the citizens of New York is to report the news accurately. If qualified journalists are not present at situations involving NYPD activity, and a mischaracterization of those events gains traction on social media, both NYPD and journalists are placed on the defensive after missing the news cycle. Journalists must then expend enormous efforts to retell the story accurately to a confused and perhaps agitated public.

NYPD and qualified journalists both require the public's trust to be effective. By working together, we can avoid the potential harms associated with the distribution of misinformation through the Internet and on social media platforms.

To achieve this objective, we must cooperate so that qualified journalists are able to accurately cover NYPD's activities. This requires access to police communications in <u>real time</u>. Encryption of <u>all</u> NYPD communications undermines this objective. Fortunately, other law enforcement departments that have addressed this issue have been able to strike an appropriate balance between protecting police communications and allowing qualified journalists timely access. We believe these examples can serve as a template for NYPD as it moves forward with its encryption plans.

2. Develop a Mutually Agreeable Protocol and Technology Allowing Qualified Journalists Access to Real Time NYPD Communications

Encryption advocates note that security is necessary to protect the safety of officers in the performance of their duties. They claim that absent some form of encryption, criminals will have access to sensitive information that could place the lives of officers at risk. In addition, they note there may be privacy concerns with allowing journalists access to certain types of information. These concerns can be addressed by developing an encryption system that ensures officer safety, protects privacy and allows qualified journalists access to certain real time information necessary for them to fulfill their mission.

A number of law enforcement agencies have enacted such systems. For example, the California Highway Patrol (CHP) decided not to encrypt its radio communications. Unencrypted CHP transmission only includes basic information. For privacy reasons, personal information, such as criminal history, is carefully guarded and provided via computers. In San Francisco, SFPD will use certain public channels to send officers to an incident, such as asking units to respond to a specific location for a report of a robbery. Other information is protected. At the conclusion of the incident, dispatchers will state on an unencrypted channel what the outcome was, for example, officers took a report or made an arrest.

Recently, the Palo Alto Police department, which had encrypted all its communications, revised its policy to allow access while protecting specific information.

This change provides the public with open access to police radio communications and enhances officer options in securing personal identifying information. The new procedures increase field personnel flexibility by providing three different options they can use to safeguard personal identifying information depending on the situation with which they are presented. Those options are a radio check that transmits only a person's driver license number, a radio check that splits

individual components of personal identifying information into separate transmissions, or a cell phone call to our 24-hour dispatch center.¹

Law enforcement agencies in Las Vegas, Nevada; Pueblo, Colorado and Decatur Illinois have reached agreements allowing credentialed media to access police communications. We believe these jurisdictions can serve as a template for New York City.

Some jurisdictions, such as Chicago, employ a 30-minute delay in providing access to information. Such a delay effectively denies qualified journalists the ability to cover live on the scene events. We believe such a policy is fatally flawed. If a dangerous situation occurs, citizens must be informed by trusted media outlets in real time. As noted above, a delay allows those with wireless devices to record the activity live and transmit possible misinformation of the event throughout the city. Delayed access to information runs counter to the objectives of the NYPD, qualified journalists and most importantly harms the citizens of New York.

We recognize there is additional "tactical" information provided over police communications during hostage situations, active shootings, riots, drug enforcement, gang activity, Emergency Service Unit (ESU) deployment and other events. In these contexts, the safety of law enforcement officers becomes critically important, and access to communications by criminal elements poses a significant problem.

Fundamentally, qualified journalists seek to maintain access to <u>real-time</u> police dispatch radio communications. This information is essential for the coverage of events throughout the city. Access to "tactical" information is worthy of additional discussion, bearing in mind the twin objectives of informing the public and protecting the safety of officers.

Importantly, our proposal would not allow criminal elements to access any such information and place officers' safety at risk. Our approach limits access to qualified journalists that have been recognized under New York Law.

3. Defining Qualified Journalists for the Purposes of Access to Police Communications

During our meeting, a question arose regarding who should be allowed to access NYPD communications. While recognizing a broader right of the public to be aware of police activities, we are proposing a narrower access policy. Under our proposal, only qualified journalists would be allowed access to the relevant police information described above. It is important to find an appropriate definition of "qualified journalist." Fortunately, New York law already has workable definitions.

Other states, such as California, have addressed this issue. In defining the persons eligible to qualify for media access, CA Penal Code §409.7 defines a qualified journalist as "A duly authorized representative of any news service, online news service, newspaper, or radio or television stations or network." New York City and New York State have also addressed this issue.

One approach would be to use the criteria that are currently used in granting press credentials in New York City. While NYPD issued these credentials in the past, press credentials are now issued through the Mayor's Office of Media and Entertainment (MOME) pursuant to Title 43 of the Rules of the City of New

¹ Press Release, Palo Alto Police Department, August 4, 2022 https://local.nixle.com/alert/9580626/?sub_id=0

York Chapter 16.² The criteria employed for issuing a standard press card for an individual or a reserve press card for a newsgathering organization would be appropriate for defining those journalists who would be eligible to access unencrypted police communications.

Another option would be to enact a standard consistent with New York State laws governing the sale of body armor. Under the New York gun law enacted last year, citizens are prohibited from the purchase, possession or sale of body armor.³ The law, however, recognized exemptions for certain professions whose jobs place them at risk. In January, the New York Department of State granted journalists and newscasters the ability to obtain body armor in New York.

The information set forth above supports a determination by the Department that the activities of the professions of "qualified journalist" and "newscaster" sometimes require members of such professions to put themselves in dangerous situations that may expose them to serious physical injury, and that such serious physical injury may be prevented or mitigated by the wearing of body armor. Based on the foregoing and the requirements of Executive Law §144-a and 19 NYCRR Part 905, the Department has designated the professions of "qualified journalist" and "newscaster," each as defined in section 79-h of the New York State Civil Rights Law, as eligible professions and adds such professions to the Department's list of eligible professions.⁴

This definition is relevant to the present situation. For public safety reasons, the New York Department of State wanted to limit the ability of the general public to purchase body armor. As a result, it was very restrictive in defining those professions, including journalists and newscasters, that would be eligible to purchase body armor.

Also, NYPD will have experience applying the new body armor standard. Under the New York gun law decisions regarding who can purchase body armor, including the scope of the journalist exemption, are to be enforced by local police departments. As a result, the definition contained in the body armor exemption for journalists will not be an alien concept. To the contrary, NYPD will have to apply this standard every day. Simply stated, if a journalist is qualified to purchase body armor, they should also be qualified to access unencrypted police communications.

Finally, this plan provides access that is limited to only to qualified journalists. It denies access to those who want to break the law or threaten the police. Under the current system of "unencrypted" NYPD communications, there are virtually no instances where a qualified journalist provided criminal elements with information obtained from police communications. Limiting access to <u>qualified</u> journalists significantly reduces the risks of sensitive information falling into the wrong hands and endangering the safety of members of the service.

² See: https://www1.nyc.gov/assets/mome/pdf/Final Press Credential Rule 2021.pdf

³ See: https://dos.ny.gov/body-armor

⁴New York Department of State, Determination In the matter of requests that "journalist," "broadcast journalist," and "news crews" be designated as eligible professions for the purchase, sale, and use of body armor. January 13, 2023, https://dos.ny.gov/system/files/documents/2023/01/determination-journalist-et-alia.pdf

Technical issues: There Will Be no Interference to NYPD Communications.

Encryption advocates argue that it is necessary to prevent individuals from hijacking or otherwise causing interference to police communications. While we do not know the technical specifications of NYPD's proposed system, we can guarantee there will be <u>no</u> interference from our proposal.

To the extent NYPD is developing a new system that is transmitting encrypted information on public safety radio frequencies "over-the-air," it will be placing numerous transmitters and repeaters at various locations throughout the city. As a technical matter, the only way there can be interference is by illegally operating and unauthorized transmitter on the same or an adjacent frequency.

But we are not suggesting that journalists have access to transmitting equipment or transceivers. We are asking to access NYPD communication by using only <u>receivers</u> that can access NYPD transmissions. Like the radio in your car, the receivers used to access NYPD communications are unable to transmit, making it impossible to cause interference with police communications.

There have been instances where police communications systems have received interference from illegal transmitters operating on public safety frequencies. Those instances do <u>not</u> involve qualified journalists who have been listening to unencrypted communications on scanning receivers for years. Those instances involve the illegal use of a <u>transmitter</u> (not a receiver) operating on police frequencies. Such illegal transmissions violate both Federal and New York State laws.

Access to information by qualified journalists may depend in part on the technical architecture of the NYPD's proposed system. For example, New York City covers a large geographic area with precincts throughout the five boroughs. It is likely that a new NYPD communications system will employ a series of transmitters that allows NYPD to cover the entire city, but independently transmit different information in each area. Depending on the geographic coverage area of each transmitter, this could require news organizations to purchase multiple receivers and place them in different locations throughout the city. Purchasing multiple radio receivers that decode encrypted communications could be cost prohibitive.

A low cost approach would be to take <u>real-time</u> NYPD communications and place them on a secure internet service such as *Broadcastify*. https://www.broadcastify.com/ Numerous police and fire departments across the country have already placed their communications on this system. Such a service would allow journalists access to NYPD communications throughout the city using the online service without having to purchase multiple receivers and place them in different locations. With an online service, NYPD could control who is able to monitor such communications by providing individually identifiable access codes.

We understand NYPD is in the process of testing its new system. At this point it is difficult to gauge the technical issues without additional information. Depending on the system's technical architecture, some of our concerns may not arise. We would like to engage in further discussions with NYPD, because the technical aspects of the system can negatively affect access by journalists.

5. Enforcement

We recognize that NYPD has concerns regarding the security of its system. There are two issues. First, how to ensure that only qualified journalists can access the information. Second, what happens if a qualified journalist misuses or allows others to access NYPD encrypted communications.

As to the first concern, we would be happy to discuss implementing data security measures. This would include access to hardware (radio receivers) or digital communications. This could include required key cards to access radio receivers in newsrooms. It could also include requiring authentication to access digital communications. Similarly, we would establish training, best practices and/or a code of conduct to help prevent improper access.

The second concern is based on trust. For years qualified journalists have worked with NYPD in a qualified and responsible manner. When given confidential information from law enforcement, we honor that commitment. The same is true for protecting confidential sources. Journalists who fail to live up to these commitments do not remain in the profession for very long. There is every reason to believe that qualified journalists will not misuse their ability to access NYPD communications. A breach of that trust will make it difficult if not impossible for a journalist to work with NYPD. Indeed, violating this trust could result in disciplinary action by their news organization.

Nonetheless, we recognize NYPD is concerned that communications received by journalists may be misused or used by non-journalists. To this end it is worth discussing administrative mechanisms that may be used by NYPD to ensure compliance. For example, depending on the technical aspects of the system being developed, it may be possible to change transmitting codes and encrypt all radio receivers used by an offending party. If NYPD uses an internet-based system, then it could deny future access by changing access codes. We are willing to discuss a range of options to address NYPD's security concerns.

6. Summary

We appreciate the opportunity to present our views regarding NYPD's proposed plans to encrypt its communications system. We hope this memorandum explains the challenges and opportunities in resolving this issue and can serve as a basis for future discussions. There is a concern that decisions may have already been made regarding the system that is in the process of being tested. We are not sure if the technical aspects of system will limit the potential options for journalists to access these communications. Accordingly, we look forward to continuing our discussion with you in a timely manner. Thank you for your consideration and we look forward to working with you and your team.

Respectfully submitted,

Bruce Cotler, President, New York Press Photographers Association
David Donovan, President, NYS Broadcasters Association
Diane Kennedy, President, NY News Publishers Association
Thomas Maddrey, Chief Legal Officer, American Society of Media Photographers
Todd Maisel, Government Relations Chairman, New York Press Photographers Association
Lloyd Mitchell, Govt. Relations Committee, New York Press Photographers Association
Mickey H. Osterreicher, General Counsel, National Press Photographers Association
Dan Shelley, President and Chief Executive Officer, Radio Television Digital News Association
Peter Szekely, President, Deadline Club, Society for Professional Journalists
Jane Tillman Irving, past-President, New York Press Club

NEW YORK NEWS PUBLISHERS ASSOCIATION, INC.

252 Hudson Ave. ● Albany, New York 12210 ● 518-449-1667 ● Fax: 518-449-5053 ● www.nynpa.com

Diane Kennedy President

Albany—Times Union

Amsterdam-The Recorder

Auburn—The Citizen

Batavia—The Daily News

Binghamton—Press & Sun-Bulletin

Buffalo—The Buffalo News

Canandaigua—The Daily Messenger

Catskill—The Daily Mail

Corning-The Leader

Cortland—Cortland Standard

Dunkirk—The Observer

Elmira—Star-Gazette

Geneva—Finger Lakes Times

Glens Falls—The Post-Star

Gloversville—The Leader-Herald

Herkimer—The Evening Telegram

Hornell—The Evening Tribune

Hudson-Register-Star

Ithaca—The Ithaca Journal

Jamestown—The Post-Journal

Kingston—Daily Freeman

Little Falls—The Evening Times

Lockport—Union-Sun & Journal

Long Island-Newsday

Malone—The Malone Telegram

Massena and Potsdam-

Courier-Observer/The Advance News

Medina—The Journal-Register

Middletown—The Times Herald-Record

New York City—The New York Times
New York City—The Wall Street Journal

Niagara Falls—Niagara Gazette

Norwich—The Evening Sun

Ogdensburg—Ogdensburg Journal

Olean—The Times Herald

Oneida—Oneida Daily Dispatch

Oswego—The Palladium Times

Plattsburgh—Press-Republican

 ${\color{red}\textbf{Poughkeepsie}} \textcolor{blue}{\longleftarrow} \textcolor{blue}{\textbf{Poughkeepsie}} \textcolor{blue}{\rightarrow} \textcolor{blue}{\textbf{Poughkeepsie}} \textcolor{blue}{\rightarrow} \textcolor{blue}{\textbf{Poughkeepsie}} \textcolor{blue}{\rightarrow} \textcolor{blue}{\textbf{Poughkeepsie}} \textcolor{blue}{\rightarrow} \textcolor{blue}{\textbf{Poughkeepsie}} \textcolor{blue}{\rightarrow} \textcolor{blue}{\textbf{Poughkeepsie}} \textcolor{blue}{\rightarrow} \textcolor$

Rochester—Democrat and Chronicle

Rochester—The Daily Record

Rome—Daily Sentinel

Salamanca—Salamanca Press

Saranac Lake—Adirondack Daily

Enterprise

 ${\bf Saratoga\ Springs} \hbox{---} {\bf The\ Saratogian}$

Schenectady—The Daily Gazette

Staten Island—Staten Island Advance

Syracuse—The Post-Standard

The Tonawandas—Tonawanda News

Troy—The Record

Utica—Observer-Dispatch

Watertown—Watertown Daily Times

 $\textbf{Wellsville} \color{red} \textbf{--} \textbf{Wellsville Daily Reporter}$

White Plains—The Journal News

Amended Testimony

New York News Publishers Association

Committees on Public Safety, Technology and Government Operations

New York Police Department Radio Encryption

Thank you for the opportunity to submit amended testimony following the Nov. 20 hearing by the Committees on Public Safety, Technology and Governmental Operations. We truly appreciate the interest and attention provided to us by the members of the Committees, and would like to provide supplemental discussion of issues which were raised during the hearing.

The New York News Publishers Association represents the publishers of newspapers throughout New York State. Our members include the largest metropolitan daily newspapers, suburban newspapers throughout upstate and Long Island, rural weekly newspapers and emerging digital news organizations.

A scanner that broadcasts police radio communications has been a mainstay of newspaper newsrooms since the 1930s. Journalists monitor scanner traffic in order to have real-time information that enables them to report on events affecting their communities, as the events are unfolding.

Real-time access to first responder radio communications enables journalists to gather immediate information about terrorist attacks, natural disasters, demonstrations, traffic accidents, structural fires and collapses, and other events that members of the public need to be immediately aware of in order to take steps to avoid being in the path of danger. Journalists themselves need to know what type of event they are approaching in order to maintain their own personal safety to the extent possible.

Further, facilitating real-time coverage of events by professional journalists can help counteract social media misinformation, which can quickly go viral due to its capacity to inspire strong emotion in viewers.

To my knowledge, access to scanner communications by journalists has never led to the injury of any first responder.

The overwhelming majority of interactions between law enforcement personnel and journalists are positive, and in fact, are beneficial to law enforcement. The capacity of journalists to show the public that law enforcement personnel are carrying out their responsibilities should help to reassure the public that first responders are on the job, performing their duties.

That said, we are all aware of incidents in which only the capture of video as an incident is unfolding has revealed wrongdoing that could otherwise have been concealed.

During Monday's public hearing, Ruben Beltran, Chief of Information Technology of the New York Police Department alluded to other jurisdictions which have either eliminated journalists' access to encrypted radio communications or provided access on a time delay. Chief Beltran also suggested access to recordings of radio communications might be provided through Freedom of Information Law requests. Lastly, Chief Beltran also remarked that journalists are resourceful people and might be able to learn about and cover events even if no access to radio communications is provided.

These statements were disappointing to hear, to say the least, and we feel compelled to respond.

1) Time delay.

As is frequently said of journalist access to government information, "access delayed is access denied." Nowhere is that more true than with respect to police radio communications, where journalists are obligated to accurately report in real time about events that could pose a serious threat to public safety. For this reason, none of the three options (time delay, FOIL or outright denial of access) would enable journalists to perform their jobs.

The City of Chicago encrypted its police radio communications in 2022, providing journalists with access delayed by 30 minutes. According to a Dec. 12, 2022 post by Fox 32 News: "The encryption is already happening. Last week, a shooting took place at a courthouse and police district in Chicago. The perpetrators fired more than 40 shots and escaped on an expressway. Chicago blocked all live scanner transmissions of this incident. Also, last week, we learned that a man armed with a rifle was walking down the street in West Pullman during dinnertime while families were returning home from work and school. We were not able to alert the public as it was happening. Again, blocked by the city of Chicago." Clearly, a 30-minute delay endangers public safety.

A 30-minute delay also imperils transparency in policing. Immediate access to radio communications has enabled journalists to publish video of the deaths of individuals at the hands of law enforcement. Publication of the video of the death of Eric Garner in July 2014 sparked public outrage and led to New York City legislation prohibiting the use of chokeholds, a law which was this week upheld by the New York Court of Appeals (82opn23-Decision.pdf (nycourts.gov).

2) Freedom of Information Request

The assertion that journalists would be allowed to access radio communications through filing a Freedom of Information Law request is even less worthy of serious discussion. At its best, a FOIL request can produce records in a matter of days. NYPD's response times are often considerably longer. Journalists and civil rights organizations frequently encounter lengthy delays in FOIL responses from NYPD, as documented in litigation filed by the Surveillance Technology Oversight Project (NYPD FOIL Noncompliance Lawsuit — S.T.O.P. - The Surveillance Technology Oversight Project (stopspying.org). "The lawsuit claims the NYPD engages in a pattern and practice of unlawfully refusing to respond to Freedom of Information Law (FOIL) requests, citing NYPD delays in 42,000 requests over the past four years. The lawsuit alleges that in 2019, the NYPD claimed more than 34 years' worth of FOIL extensions, but by 2021 the number grew to more than 50 years' worth of delays."

3) Refusal of Access

Lastly, the contention that journalists are resourceful and would be able to work around government blockades of access to information is perhaps the most distressing, for its cavalier dismissal of the role of the press in reporting on government activities.

At least two jurisdictions have decided the cost in transparency raised by encryption that would eliminate press access outweighed the perceived benefits.

In 2023, the City of Palo Alto, California rescinded its encryption policy (<u>Palo Alto police set to remove radio encryption | News | Palo Alto Online |</u>). Notably, Palo Alto was able to overcome the issues of personal privacy (in which medical, age, home address or other information about victims, bystanders or others might be publicly revealed via unencrypted radio communication) which have been raised as a barrier by NYPD.

Las Vegas opted to provide journalists with access to encrypted radio communications, and the experience has been positive, as detailed in a January 17, 2023 letter to Chicago Mayor Lori Lightfoot from the Chief Legal Officer of the Las Vegas Review-Journal:

"LVMPD expressed several concerns as justification to implementing encryption, including officer safety, public safety (e.g. not permitting criminals to gain an advantage against law enforcement by listening to communications), and issues regarding privacy. However, when LVMPD began encrypting its communications, the department nonetheless made an accommodation for members of the media to continue to receive real-time access to police communications by allowing media organizations to purchase radios capable of unencrypting the communications. The City of North Las Vegas also allows the media to receive access to police communications. The Las Vegas Review-Journal is one of the media outlets that has such real-time access to police communications from LVMPD and the City of North Las Vegas.

Our first-hand experience with this arrangement over the past five years has been unproblematic and the relationships between LVMPD and the media and the City of North Las Vegas and the media has not been negatively impacted by permitting media access to the communications. We know of no compromise of officer safety resulting from media access.

Likewise, we are unaware of any incident where access resulted in a breach of privacy or a threat to public safety. To the contrary, the ability to continue to receive communications in real-time enables the Las Vegas media to continue its important role in keeping the public informed of dangerous situations and ensuring public safety. We have had no security issues regarding either unauthorized access to the radio equipment itself or to information obtained from the radio communications for nefarious purposes."

We urge the City Council to enact legislation granting journalists real-time access to police radio communications that are not tactical or which would reveal private details of individuals. Journalists could apply for a secure method by which to access transmissions.

In order to ensure that only genuine journalists have access to radio communications, the city should adopt a system granting journalists, as defined under Sec. 79-h of New York State Civil Rights Law, access through a secure connection. This would be akin to the current state regulation that permits

journalists to purchase body armor, which is administered through the New York State Secretary of State's Office and enforced by local police agencies, including NYPD.

The pertinent language in 79-h of NY Civil Rights Law reads as follows:

(6) "Professional journalist" shall mean one who, for gain or livelihood, is engaged in gathering, preparing, collecting, writing, editing, filming, taping or photographing of news intended for a newspaper, magazine, news agency, press association or wire service or other professional medium or agency which has as one of its regular functions the processing and researching of news intended for dissemination to the public; such person shall be someone performing said function either as a regular employee or as one otherwise professionally affiliated for gain or livelihood with such medium of communication.

As I and other news organization representatives mentioned during the hearing, we began a good-faith effort to collaborate with NYPD in January 2023. At NYPD's request, we submitted a briefing paper setting forth our position and suggestions for a workable solution that would preserve journalist access to the radio communications which are vital to our work, while also safeguarding law enforcement personnel. Our ongoing efforts to continue those discussions have been met, at best, with expressions of mild interest, but for the most part, with silence.

I thank you for your interest in this important matter and look forward to further collaboration with you to enhance the transparency the residents of New York City deserve.

Respectfully submitted,

Diane Kennedy

President

November 22, 2023



New York Press Photographers Association, Inc.

Church Street Station P.O. Box 3346 New York, NY 10008-3346 (212) 889-6633

http://www.nyppa.org

E-mail: office@nyppa.org

November 20, 2023

My name is Bruce Cotler, President of the New York Press Photographers Association — NYPPA; I'm here on behalf of our organization to make our stance on this matter clear. Thank you to the Council for hearing our concerns

The NYPPA is opposed to a blanket police radio encryption effort. We are sympathetic to the issues that the NYPD face, however, we are concerned about the matter of transparency should total encryption come to pass. The public has a right to know what occurs when a crime is committed, and the media is a necessary check to ensure some measure of that aforementioned transparency.

In cases such as Amadou Diallo, Sean Bell, and Eric Garner, the media was vital in providing insight as to what really occurred at the time of the incidents. Should this encryption measure pass, it will negatively affect the community, the media, and run counter to Mayor Adams' stated vision for a transparent administration. We believe that this situation can be remedied by allowing media access to monitor encrypted channels, in order to continue to serve the public good. We certainly respect the concerns of city police for security, but that must not come at the cost of transparency to those they must protect.

Sincerely, Bruce Cotler President, New York Press Photographers Association Written Testimony for the Committee on Public Safety (Jointly with the Committee on Technology and the Committee on Government Operations on Nov. 20, 2023

I write to submit testimony to the New York City Council committees named above as a member of the Board of Trustees of the New York Press Photographer's Association.

I oppose the blanket encryption of the NYPD radios for the following reasons:

- Encryption will eliminate real-time access for the news media to understand what is going on In New York City with regard to police action and responses, and limit the information on events to only what is released by the NYPD. This, in turn, will also deny access to millions of New Yorkers who depend on the media to report what's happening in their neighborhoods. Spot news coverage is a staple of media work. It provides jobs. It informs the public and it provides transparency. I would also contend that information gained through the media can help the police by allowing the public to also pass tips along to authorities. You can't "say something" if you can't "see something," or at least know what's going on. This action will also erode trust in the police.
- The media are often led to other stories beyond what happens at a spot news scene. Digging deeper into why and how something happened can often shed light on instances where our city failed, or also did its best, to protect or care for people who have been neglected or injured.
- While the NYPD may have been planning this for some time, it seems to be a surprise to many that this large expenditure is being made, specially at a time of proposed severe budget cuts. The council, as the voice of the citizens of New York City, needs time to study how these funds are being spent. Did the Council allocate them? Was the Council kept in the loop about these fund's use? Oversight it a key responsibility of the Council. It also might be helpful to inquire about other city agencies plans to use encryption.
- NYPD officers deserve to be safe. And encrypting radio communications among tactical, or other sensitive operations makes sense. It would be helpful if the NYPD if it could tell the Council about instances in which they believe that their open communications have endangered officers. Solutions to providing open transparency of the NYPD responses via their radio transmissions exist. Implementation requires consultation with the media and the public, who also have a right to listen. It can't include a system that sends information hours after an incident. A one-minute delay might be reasonable. And it will mostly likely include the need for city or state laws that regulate how the media are allowed to hear the day-to-day responses by the police rather than arbitrary police rules.

I understand the hearing may also touch on the press credentials process, which the Council removed from the NYPD and handed over to MOME. If the NYPD is concerned about who is getting press credentials, they would certainly be able to assist MOME with the background checks on press card applicants, as they used to do, and forward those results to MOME as part of its consideration for granting credentials.

Thank you for your work on this important matter, and for the opportunity to submit testimony.

Porter Binks

Member of the Board of Trustees of The New York Press Photographer's Association.

RTDNA/Encryption Testimony

Members of the New York City Council, I represent the Radio, Television, Digital News Association (RTDNA). We are the world's largest professional organization devoted exclusively to broadcast and digital journalism. Founded in 1946, RTDNA's mission is to promote and protect responsible and truthful journalism.

I come before you with more than 40 years of experience in the news business covering New York City. I spent 20 years as a broadcast reporter (WCBS880 and ABC News) and 20 years as a news manager (WCBS Newsradio 880). I speak from experience of covering news in this city and managing news coverage here.

I am here to express our deep concern about what is going in at the NYPD with respect to radio encryption. In some ways journalists and law enforcement are partners. We both serve the public. We both work to make our communities better. We both benefit from a more informed public. The public needs to know, and in fact, deserves to know what is happening in their communities especially when it relates to public safety. Encryption throws a veil over public information and the needs of informed communities.

There is no question that police, government, and even we in the media are suffering from a crisis of confidence from the people we serve. In the journalism business we know that transparency is one way to help solve the issue. In journalism we also have a saying "Be Afraid of the Dark". It means that when bright lights shine on institutions like government, like the media, and yes, the police, citizens can have a better view, a clearer picture. Encryption turns the light to dark. Encryption allows for bad players to operate in the shadows. Encryption prevents citizens from knowing what is happening in their neighborhoods in real time.

Encryption also sends a terrible message to the public. New York City should be a leader in issues related to public safety and equity. By hiding all of its operational transmissions, the NYPD is sending a signal that transparency is not important. That sets a very dangerous precedent. The domino of distrust has a long tail.

We believe its wrong-headed to shut out the media and public from police operations with encryption. We recognize that the NYPD has concerns about it and we have expressed our desire to work with them on ways to make it work to satisfy those concerns. Up to this point, we don't feel they are interested in working with us on a solution. Today, we believe the solution is you.

Respectfully

Tim Scheld Chair RTDNA

Radio Television Digital News Association | RTDNA

To the Committee on Public Safety:

My name is Gretchen Viehmann. I am a native New Yorker who is currently the Course Leader for the one of the most highly-respected photojournalism courses in Europe, Press and Editorial Photography at Falmouth University in Cornwall, United Kingdom

Before taking on this role I was the Director of Photography for the New York Daily News and before that the Director of Photography for the New York Post so I am writing from a position of deep understanding of the importance of preserving this access. Previous to these roles within the New York media, I worked in the photo collection of the Museum of the City of New York, where the ground-breaking images of Jacob Riis that exposed the conditions of the poor in New York City form the backbone of a collection that celebrates the importance and absolute necessity of the freedom of the Press.

I am appalled and dismayed by the prospect of the encryption of police radios in New York City. In my many years of experience I know how essential it is for this information to be available to members of the Press. Encrypting the radios serves no purpose other than to allow the concealment of truth from the public and to prevent the Press from doing its duty and reducing public information to a tightly controlled press release.

The long and proud tradition press freedom in New York City is under threat and the encryption of the radios must not be allowed to happen.

I currently live in a country where all emergency services radios are encrypted and I can tell you, unhappily, that the result is a press that is tightly controlled and where much information is concealed from the public. This cannot happen in New York.

Sincerely,

Gretchen Viehmann St. Hubbins House Fowey Cornwall UK PL23 1BN



Statement for the New York City Council Committee on Public Safety for its Nov. 20, 2023 Oversight Hearing on NYPD Radio Encryption held jointly with the Committee on Technology and the Committee on Government Operations

The Deadline Club is the New York City chapter of the Society of Professional Journalists, the country's oldest journalism organization with a membership of more than 4,000 and a mission that includes promoting the free flow of information to an informed citizenry.

The Society's Code of Ethics has been the news industry's most widely accepted moral guidepost for more than 50 years. Among its planks are:

• Recognize a special obligation to serve as watchdogs over public affairs and government. Seek to ensure that the public's business is conducted in the open, and that public records are open to all.

This foundational tenet of the Society is directly at odds with the New York Police Department's yet-to-be defined plans, which are already being implemented, to deny the public and the press access to its radio transmissions by encrypting them.

Encrypting NYPD radio transmissions would shroud the activities of one of the city's key public agencies in an opaque fog. News vital to New Yorkers – civil unrest, hostage situations, active shooter incidents, manmade and natural disasters – would be suppressed at the moment they need it most. If news of these events finds its way into the public domain at all, it would be well after the fact and at the discretion of NYPD public information officers.

Worse, a police radio blackout, or even delayed transmissions, could lead to the spread of misinformation. Journalists are trained to report news accurately and quickly. But just because news crews, photographers and reporters aren't at a major crime scene that the NYPD has kept under wraps doesn't mean that other people won't be there. That would leave the initial reporting of such events to a random gathering of people who are untrained in reporting, but equipped with cellphone cameras and the ability to add commentary on social media that may or may not comport with the facts.

It was access to police radio transmissions that enabled journalists to quickly respond to and report countless breaking news stories, including the September 11 attacks, the 2016 Chelsea bombing and the chokehold death of Eric Garner.

Several police departments across the country have already confronted the encryption issue with mixed results. Some have declined to go ahead with it, others have kept the press plugged in while others have closed off their communications or put them on a 30-minute delay.

As the largest U.S. police force, the NYPD wields influence beyond the five boroughs. It is therefore disturbing, not only for the city but the entire country, that the NYPD has already blacked out its communications in 10 Brooklyn precincts. The NYPD has been less than forthcoming about how it plans to continue its encryption rollout.

It's not as if New York's journalism community hasn't tried to find common ground with the NYPD.

Aware that encryption was being planned, representatives of several press organizations in the city, including the Deadline Club, met with NYPD officials in January to register our concern and gather facts. The officials asked our group, known as the New York Media Consortium, to make our case in writing, which we did in February. In return, we got very little information about how or when the encryption project would be handled or what was driving the decision to launch it, other than some vague concerns about security.

It's not easy for one party to find a solution for another party's problem when the problem hasn't been adequately defined. But we tried. Although our preference would have been to keep radio transmissions open to all, as they have been for almost 90 years, the Consortium offered options. Those options included streaming police communications through an online platform where real-time access to outsiders could be restricted to qualified journalists.

Defining "journalist" is always difficult and never perfect. Fortunately, New York State already has definitions of "journalist" and "newscaster" that have worked adequately for decades. They're found in subdivisions 6 and 7 of Civil Rights Law - CVR § 79-h, commonly known as the Shield Law, which exempts these news professionals from being cited for contempt for refusing to reveal confidential sources. The state adopted the same definition late last year when it exempted journalists and newscasters from the newly enacted ban on the sale of body armor.

The same definition also could be used to determine who gets access to NYPD radio transmissions if they become encrypted.

Since our initial meeting in January, Consortium members have been unable to reestablish contact with the NYPD, despite having spelled out our concerns and offered solutions in what we hoped would be an ongoing dialogue.

In the interest of finding an amicable solution, we have shown a willingness to give deference, up to a point, to the NYPD's expertise in maintaining public safety and security. But that deference cannot come at the expense of the public's right to know about the activities of the country's largest police force. In the inevitable tension between society's needs for information and for security, a truly free society requires that priority go to the former.

The Deadline Club opposes any restrictions on access to the NYPD's radio transmissions beyond those that the Consortium has already offered and urges the City Council to take all steps necessary to preserve and protect the public's right to stay informed of NYPD matters.

Respectfully submitted,

Peter Szekely President The Deadline Club/New York City Chapter, Society of Professional Journalists Nov. 20, 2023



----Original Message----

From: Black Radio Network <news@blackradionetwork.com>

Sent: Monday, November 20, 2023 1:51 PM

To: Office of Correspondence Services < OfficeofCorrespondenceServices@council.nyc.gov>

Subject: [EXTERNAL] Police encryption

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe. Report suspected phishing emails with the Phish Alert Button or forward them to phish@oti.nyc.gov as an attachment.

Black Radio Network fully supports the New York Press Club's strong opposition to the possible encryption of the police radio. This possibility is appalling to the free press and access to vital reporting. This is especially disturbing in the city where John Peter Zenger fought for an unfettered press. Shame on this possibility. Black Radio Network by Jay Levy

Dakota Santiago

Freelance Photojournalist

Topic: NYPD Encryption

Good afternoon, my name is Dakota Santiago. I am a photojournalist who currently works overnight as a news stringer for broadcast media and print. My sense of purpose, work wise, lives and dies with the scanner. The scanner is the equalizer of my field. I would love to be a staffer somewhere but sometimes when it's not your time yet, it's not.

And so I depend on the scanner to deliver the details needed before committing and jetting off to what members of the public should know happened overnight while they slept. Was someone shoved into a moving train, were innocent children shot at a holiday BBQ in a park, were swastikas painted into the ground of a local Brooklyn park, or were people senselessly assaulted on the basis of hate on the street for a conflict happening thousands of miles away. All these samples I just gave are all stories I've run on at least once in my years covering the beat.

All of those samples would not be news on the day of their occurrence, if at all, if the police radios were allowed to be encrypted. As things stand currently, the NYPD does not announce most newsworthy events that occur throughout a day

unless we're talking events like confirmed homicides, which most of the time reach our desk anywhere from six hours to several weeks after the incident occurred, leaving us, most often, with no evidence of a scene at all to photograph. This is why we can ill afford to lose real time access to police radios, there is nothing easy about witnessing most of the mayhem that occurs in town that often can lead to the loss of life.

What's easy is the ability to evoke a sense of false security when there is no visual evidence of the violence that goes on daily on our streets. You rob the community of their power to demand patrols, more funding, and changes in strategy or the police department itself when the public is not properly informed en masse of things that may be going sour on their streets.

The invitation for misinformation is also given the greenlight when only one entity is allowed to dictate the events of a matter. If Harlem had been encrypted in July instead of Brooklyn, we wouldn't know to ask DCPI about the 13-yr-old shot in the pre-dawn hours of July 4th, this year, that came over as a 10-13 (NYPD Code For Backup/officer in distress) in this case, a call for crowd control at 310 W. 143rd St, the 10-13 was broadcasted on the still open citywide frequencies but you had to be listening to the division radio, in this case, the confines of the 32nd Precinct, to have heard the reason for the commotion was a young teenager, innocent victim, shot in the leg. No citywide channel like the Special

Operations Division, that we depend on for the majority of calls we respond to ever repeated a level 1 mobilization for a person shot, let alone confirmed shots fired. There would've been a child shot in that community that morning and no one but who was there would have known because he was going to survive his injuries.

City Wide 4 used to be a frequency we could listen to before it was encrypted over the spring which featured the robbery divisions of the NYPD that have the okay to conduct extended high speed pursuits across the city that often cause crashes or pedestrian strikes, we can't hear anything from them anymore.

I just got back from San Francisco where a crazed man, on October 30th, 2023, led the SFPD, an encrypted department, on a pursuit while tossing live pipe bombs out his car window that exploded in the areas of Nob Hill and downtown, near city hall. When I interviewed and spoke to residents hours after the bombs exploded they all replied with the same answer, they had no clue the explosions they heard outside their apartment buildings or in their nearby neighborhood were legitimate bombs going off.

That's not what we need here. I spoke to a contact at a Bay Area affiliate news station that told me the argument for encryption was officer safety there as well.

What about public safety, the chance to alert residents of an area in a timely matter, when bombs are literally blowing up in the street, do we want that?

The move to encrypt is the most regressive policy the city can allow the NYPD to implement especially in this day and age where misinformation is extremely volatile and effective. The NYPD states they are also moving towards encryption to keep private information off the air but what they failed to mention at the hearing was that they already have a protocol for handling sensitive information and that's by using their department issued cell phones and computers in their vehicles, you'll hear the code "10-3" spoken over the air when they order units to send information via a cell phone call instead of over their radio. They also did not inform us at all of encryption in the current 10 precincts, the Brooklyn North analog radios worked one night in July and died the next.

CITY COUNCIL OF THE CITY OF NEW YORK
COMMITTEE ON PUBLIC SAFETY
PUBLIC HEARING NYPD ENCRYPTION, PRESS CREDENTIALING
Nov. 20, 2023

TESTIMONY OF JASON B. NICHOLAS, Journalist

I have been a working New York City journalist since 2006. I brought the federal civil rights lawsuit that motivated this council to pass legislation in 2021 moving press credentialing authority from the NYPD to the Mayor's Office.

One thing I've learned in all those years is that Government accountability is necessary for Government to function optimally. When it comes to the NYPD, accountability starts with being able to listen to its radio broadcasts—as journalists in New York City have been able to do for almost 100 years without the sky falling.

Cloaking the NYPD's radio broadcast in secrecy will result in loss of accountability which translates into innocent citizens killing by unjustified or excessive police force. It also translates into unjustified police tactics like stop-and-frisk that violate New Yorker's civil rights wholesale.

News photographers would be particularly impacted by encryption. While reporters may be able to piece together a story in reverse, photojournalists can never travel back in time to replicate an image they weren't there to capture when it happened.

The power to be there—and be there within minutes—is what close and careful surveillance of police radio transmissions captured by a scanner gives journalists. No other news gathering method or technology comes close to duplicating it.

I urge the City Council to enact legislation legally requiring the NYPD to not digitally encrypt its radio broadcasts so that the public can monitor, for itself, how its police department works.

Alternatively, I urge the City Council to enact legislation requiring the NYPD to allow journalists credentialed by the City to listen to even encrypted NYPD radio broadcasts, so that the press can continue to serve its vital role as guardian of liberty.

Hello,

I'm writing to express my alarm at the NYPD's plan to encrypt radio transmissions, thereby prohibiting journalists and the public from accessing transmissions. It is critically important that the press and members of the public, who interact with police officers on a daily basis, be able to access the crucial information that comes from these transmissions. The NYPD has a long history of secrecy and abuse, showing over and over again that it cannot be trusted to oversee itself. This attempted move reflects more of the same. The public and the press deserve—and we demand—more transparency and accountability from the NYPD, not less.

Thank you,

Jillian Steinhauer, NYC journalist

Radio Encryption Battle Letter by Lloyd Mitchell

The media is not against officer safety. In fact we want officers to go home to their families at the end of their tours. What my fellow media members and I are against is the NYPD's ability to control the narrative on important stories involving their agency and affecting local communities.

Radio encryption effects people from disadvantaged communities in these ten areas, that the radios are dark let alone going forward across the city. Radio encryption will not keep families safe as they walk to school in crime ridden areas.

It will provide heartache after their child is shot. The communities won't know because it won't make the news cycle. For example on August 21, 2023, a 24 Year Old man was fatally shot by a 15 year old teen in East New York deli. A story never made the local news cycle.

Reporters are supposed to help the police get the word out. We can't get the word out if we are encrypted. That does a disservice to communities, news outlets and NYPD.

Martin Grillo EMT-P, CIC PO Box 116 Howard Beach NY 11414 ###-###-#### INFO@EMRNYC.COM

My name is Martin Grillo, and I have served New York City for over 45 years in various capacities as a Volunteer EMS Provider, Volunteer Firefighter, Voluntary Hospital Paramedic, New York City EMS Paramedic and in Law Enforcement.

I am a NYS Paramedic Instructor.
I am also recognized by New York State as a: Communications Leader Instructor,
Communications Technician,
Incident Communication Center Manager,
Incident Tactical Dispatcher,
Radio Dispatcher,
Auxiliary Communications Instructor,
I am also an FCC licensed radio technician.

I am here to speak against New York City Police Department, Fire Department and EMS encrypting their radios.

As a responder to the 1993 World Trade Center bombing and the World Trade Center attacks on 9/11 and various major emergencies, including multiple plane crashes. It is imperative that all agencies work together seamlessly and be able to be interoperable. That is one of the keys that were brought up in the 9/11 commission report.

Over the years agreements were made between volunteer first response agencies to sign out police radios from precincts until police officers were issued their own radios, then other arrangements were made so the volunteer ambulance and fire agencies can be able to monitor the police frequencies to respond and help quickly in time of need.

One incident In particular was how one of the Volunteer Ambulances in New York City were first on the scene at the shooting in Bedford Sty of two police officers, and were able to give them aid almost immediately after the incident. This is just one of many incidences were timely info from the police radios was used to save lifes.

I personally was at Flight 587 that crashed in the Rockaways, less than five minutes after the crash after hearing of the incident over the police radio, with the local Volunteer Fire Department. Unfortunately, there was massive loss of life, but we were there if there was any possibility of taking care of survivors.

Any delay in receiving the transmissions from the NYC public safety agencies would cause a delayed response of

Martin Grillo EMT-P, CIC PO Box 116 Howard Beach NY 11414 ###-###-#### INFO@EMRNYC.COM

the Volunteer First Responders in New York City to be able to respond in a timely manner to protect their communities.

The other issue is a technical issue. The police department is switching over from an analog radio system to a digital radio system. Digital radio systems inherently are either on or off. You either hear a signal very well or you hear no signal at all, while an analog system, which is currently being used as much safer because The dispatcher might hear a scratchy signal or someone trying to call for help while a digital signal, nothing possibly would be heard.

Unfortunately, an incident in Washington DC during an operation with DC Fire due to the failure of the radio system that was using digital encrypted radios contributed to loss life. Since then DC Fire is no longer using encryption.

I do believe there is a use for encryption for sensitive law enforcement operations, such as warrants, or other high risk law enforcement operations, but for day-to-day operations, there is no reason that the citizens of New York, as well as the Volunteer Emergency Service personnel should be locked out of being able to monitor the New York City public safety agencies.

Thank you for allowing me to time to express my professional opinion that New York City Public safety agency should not be using encryption for day-to-day operations. Feel free to contact me if need any further information.

Martin L. Grillo EMT-P, CIC, EMC COM L Inst. / ITSL(t) / COM T / INTD / INCM / RADO / AUXC Inst PGGB063396 / GROL/ R To whom it may concern,

Since March 2023, I've been harassed and coerced by local, state and government entities. Hacking my phone, and laptop- as well as tracking me via GPS- without reasonable cause.

I've reported my grievances to local and federal authorities:

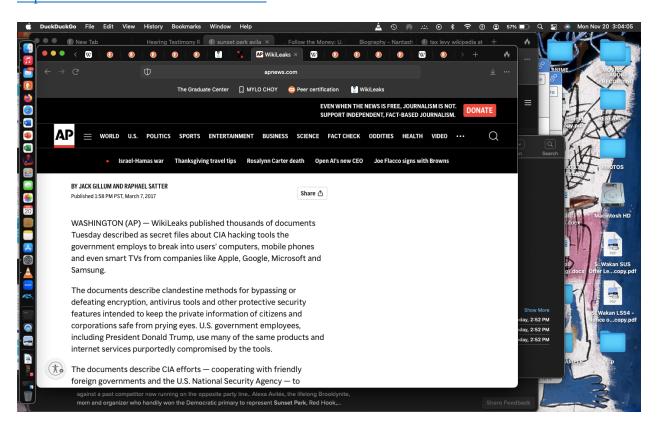
New York Police Department: <u>SAMMY.KWAN@nypd.org</u>

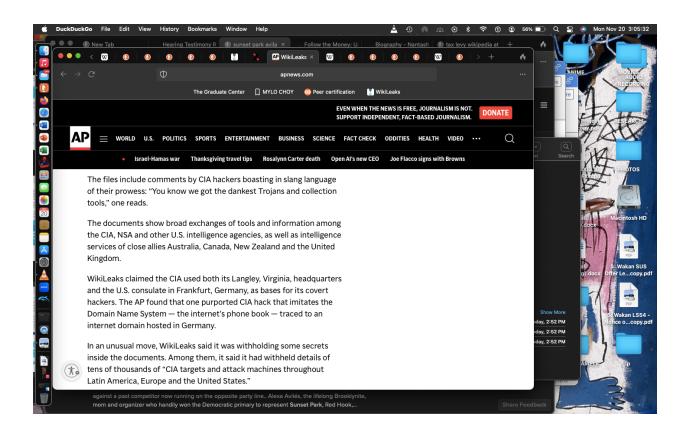
Federal Bureau Of Investigation: Investigation number #8005

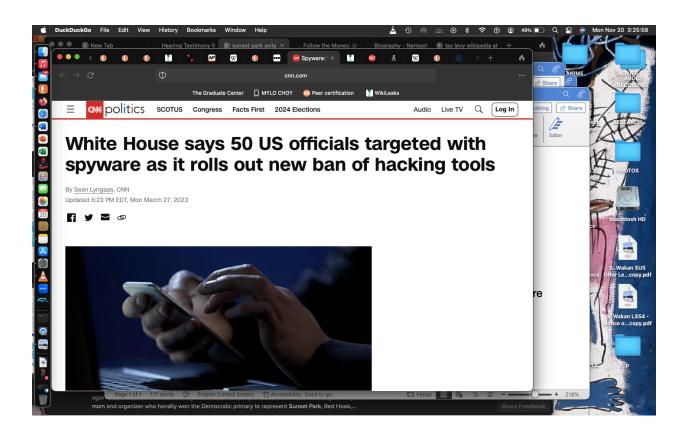
Regardless of my complaints, nothing has been done. There has been no follow up.

How can there be a just investigation practicing integrity, when the leaders of the entities I identified, are affiliated with a secret society. And utilize illegal methods to stalk, harass, intimidate and coerce private citizens. This is becoming more and more evident based off of current events:

https://ddosecrets.com/wiki/BlueLeaks







This is a global issue, in which international entities are exchanging information to exploit local citizens. An example, local American police agencies are coordinating with companies in Germany to buy hack ware to use upon US citizens unconstitutionally.

There are no laws PROTECTING INDIVIDUALS from hackers, either private citizen hackers or public entities such as police.

Political activist such as Blacklives matter groups and the George Floyd protesters were hacked for publicly gathering and for internet searches relating to the aforementioned entities and individuals:

https://www.pasadenanow.com/main/supporters-of-jailed-black-lives-matter-organizer-accuse-pasadena-police-of-surveillance-harrassment-brutality

Richards states "The Pasadena Police Department and its prosecutors are ... terrorizing the community," Gyamfi said. "With intimidation, with violence, with false arrests, with false imprisonments, and retaliatory prosecutions that are being used to kill free speech and criminalized civilians who are struggling for the right to be human, right here in Pasadena."

https://www.nytimes.com/2022/07/10/us/politics/defense-firm-said-us-spies-backed-its-bid-for-pegasus-spyware-maker.html

https://www.aljazeera.com/economy/2023/6/15/us-government-agencies-hit-in-global-hacking-spree

#BlueLeaks and the defund the police movement (The Police and criminal justice system needs to be defunded not solely for brutality, moreso secret society protection, it's being used as a tool for organized crime for secret societies. This is why police must be defunded)

The police being used to coerce, blackmail, extort, intimidate, and falsely imprisoned- is due to secret societies attacking innocent private citizens.

This is a constitutional coup- being demonstrated upon me and many other individuals around the world- in an attempt to isolate us and disenfranchise us. To attack free speech and publicly gathering for events not orchestrated by secret societies practicing Hegel's methods of "Thesis, Antithesis, and Synthesis." Manipulating both sides of a controversy for control.

I am not seeking to join any secret society- to benefit from the exploitation of the poor and at-risk populations, of which I've served for my entire working career.

Sincerely,

Shahar Wakan

Testimony to the City Council on Radio Encryption

This is not about radio encryption, it's whether you TRUST the NYPD? Do you trust the NYPD controlling the narrative? Do you trust police to be 100 percent honest, fair, and transparent with the most regressive transparency policy in the history of NYC – something you are presiding over at this very moment?

The NYPD academy instructors specifically teach cadets that "we" the press are the enemy, right out of the Trump playbook. You approve their budget every year with scant questioning of motivations and tactics. This is under your roof.

They claim encryption is about safety and will give some sort of access to the media. Since July 17, the entire Brooklyn North area is dark. 2.5 million Citizen App followers no longer get information on those communities. Breaking News Network no longer gets timely info. The press has been locked out with no date set for giving access, despite their promises. Instead of making the public safe, the public is less safe as the NYPD covers up crime in the highest crime areas of Brooklyn.

They do send out emails. One double homicide on Sept 9, wasn't reported until Saturday morning sept 14. Other crimes have taken up to a day before anything is known. Is it possible that the 73 & 75 precincts had no shootings or homicides in two months? Do you trust the police?

The Eric Garner video would've been gone if a Daily News photog hadn't heard the cryptic radio calls attempting to cover up the death. His killer, Panteleo, took 5 years to be fired by the NYPD. Do you trust the cops?

Remember Justin Volpe and what he did with a plunger to Abner Louima in a precinct stationhouse? A cop doesn't have to be a particular color – witness the 5 Tennessee cops who killed Tyree Nichols. Cops are cops – they are human and because they are armed and have incredible power, they need checks and balances – something encryption eliminates. You will only know what they want you to know.

Four years ago, I covered a crash in Flatbush in which an alleged drunk driver killed a young woman and injured her friend. The driver was a cop – nobody did a

breathalizer, the reports were hidden and the DA refused to prosecute, under NYPD pressure. Do you trust the cops?

If you give them this power, not require them to explain what they plan, when will they give press access and to what frequencies, you can't trust them. Their plan was to give us nothing otherwise in the six years they been working on this, spending more than a billion dollars. The plan was to have no plan – we know.

At the moment, the NYPD fails to provide adequate or timely info on many incidents. They fail to honor legal FOIL requests because there are no personal repercussions. I've had more than a dozen FOIL requests rejected or put off for years. They don't want you and me to know what they do.

And the NYPD is laughing at your decision to change the credentialling to MOME – something they are now using against the press.

This is on you today. All the work you've done under BLM banner, all the efforts you made on the Post Act that they fail to abide, all you've done to make the NYPD a great department, will be for naught if you drop the ball. When things go wrong at the NYPD, it will not be on them, it will be your fault - everyone will remember. I ask you to do the right thing and hold the NYPD feet to the fire.

Todd Mark Maisel

As a NYC resident and a student journalist, I was very upset to hear of the NYPD's intentions to close off radio transmissions to the public. In addition to blocking journalists from reporting on breaking news on police scenes, I believe that this plan would contribute to a greater divide between the police and the community, further inhibit trust in the police, and prevent accountability. As a resident of New York City, I hope to see greater transparency and communication from the police, not less. As a student journalist, I am concerned by the prospect of journalists being required to rely on NYPD press releases for accounts of breaking news. I believe that allowing breaking news to be filtered through the NYPD's press department and not by objective observers harms the relationship between police and civilians and leaves concerning gray area for inconsistencies. This is a matter of concern for me and I plan to remain involved in this issue for the good of the community.

•	Appearance Card			
	speak on Int. No Res. No in favor in opposition			
	Date: 11/20/3023			
2 1 1	(PLEASE PRINT)			
	Santiago			
Address:	10. C Bayonne, NJ 07002			
I represent:				
Address:				
THE COUNCIL THE CITY OF NEW YORK				
	Appearance Card			
I intend to appear and	in favor in opposition			
Address: 1330 Au	Date: (PLEASE PRINT) - CAMP - CLS 38+ AL - CLM			
	THE COUNCIL			
THE (CITY OF NEW YORK			
	Appearance Card			
I intend to appear and s	peak on Int. No Res. No			
<u> </u>	in favor in opposition Date:			
M. H	(PLEASE PRINT)			
Name:	Green Valley Rd			
1 Topicsont.				
Address:	3			



Appearance Card				
I intend to appear and speak on Int. No Res. No				
Date: 11/20/23				
Name: M SCHED PRINT)				
Address: N/C N/				
I represent: RTONA				
Address: Washington DC Basis				
THE COUNCIL THE CITY OF NEW YORK				
Appearance Card				
I intend to appear and speak on Int. No Res. No in favor in opposition				
Date:				
Name: LIOY d MITCLE/				
Address: 10/60klyn				
I represent: Myselx and other Journalist				
Address:				
THE COUNCIL THE CITY OF NEW YORK				
Appearance Card				
I intend to appear and speak on Int. No Res. No				
in favor in opposition				
1) 10. 2015				
Date: 11 . 20 - 2023				
Name: Bruce Coffee				
Name: Bruce Cotter Address: Brighen St				
Name: Bruce Cotler				

Please complete this card and return to the Sergeant-at-Arms

Appearance Card				
I intend to appear and speak on Int. No Res. No				
in favor in opposition				
Date: Nov. 20, 7023				
Name: DAVID L. DONOVAN				
Address: 1805 Western AUE Albert NY				
I represent: WY SINTE BIONDIASTERS ASSN. THE				
Address: SAMP				
THE COUNCIL				
THE CITY OF NEW YORK				
Appearance Card				
I intend to appear and speak on Int. No Res. No				
in favor in opposition				
Date: Nov. 70, 2013				
(PLEASE PRINT)				
Name: Jerry Clase, Davis Wyl- Treva ell				
Address: 1751 Aven of the Americas, New York, NY 10020				
I represent: ASC NOWS & WARC				
Address:				
THE COUNCIL				
THE CITY OF NEW YORK				
THE CITTOF NEW TORK				
Appearance Card				
I intend to appear and speak on Int. No Res. No				
in favor in opposition				
Date: (20 / 23				
(PLEASE PRINT)				
Name: Dravo Annio Alban and				
Address: ADZ HOSDON ACK, HILL AND GIVE				
I represent: 14 4 May 100 (13 MC/3 436)				
Address:				



Appearance Card I intend to appear and speak on Int. No. _____ Res. No. in favor in opposition (PLEASE PRINT) Address: I represent: Address: THE CITY OF NEW Appearance Card I intend to appear and speak on Int. No. _____ Res. No. in favor in opposition Address: I represent: Address: THE COUNCIL THE CITY OF NEW YORK Appearance Card I intend to appear and speak on Int. No. _____ Res. No. _ in favor in opposition Date: _ Address: I represent: Address:



Appearance Card I intend to appear and speak on Int. No. _____ Res. No. ____ in favor in opposition Date: I represent: FREEDOM NEWS TV Address: THE COUNCIL THE CITY OF NEW YORK Appearance Card I intend to appear and speak on Int. No. 096 Res. No. in favor in opposition Date: (PLEASE PRINT) Address: ______ THE CITY OF NEW YORK Appearance Card I intend to appear and speak on Int. No. _____ Res. No. _ in favor in opposition Date: ____ | (PLEASE PRINT) Name: Address: I represent: MOME PCO Executive Address: Please complete this card and return to the Sergeant-at-Arms

	Appearance Card			
Lintend to annous and	eneck on Int No.			
	in favor in opposition			
	Date:			
01	(PLEASE PRINT)			
Name: Sas	SKARDO, ESR			
Address:	senior Counsel			
I represent: MO	ME			
Address:	Centre St.			
	THE COUNCIL			
THE CITY OF NEW YORK				
Γ		7		
	Appearance Card			
	speak on Int. No Res. No			
	in favor in opposition			
	Date: 11/12-01/6-53	_		
Managin	a Attorney Juliane Farruggio	P		
Name: Managin	3 ATTOMEY JOI and Fall Oggic	_		
Address:		_		
I represent:		_		
Address:		_		
	THE COUNCIL			
THE (CITY OF NEW YORK			
	Appearance Card]		
I intend to annear and s	peak on Int. No Res. No	7		
i i	n favor in opposition	-		
	Date:			
	(PLEASE PRINT)			
Name: Brenna	Lip			
Address: EZ	nd 5-trec+ 10003	- 4		
I represent:				
Address:				



		production of the same of the
	Appearance Card	
Lintand to announ and	speak on Int. No.	Res No
	in favor in oppositi	on
Ш	ravor m oppositi	11/20/2023
		11/20/2000
Name: ANDAEW	(PLEASE PRINT)	
A THEADON	1085	
Address:	NYPN	
I represent:		
Address:		
STATE OF THE STATE	THE COUNCIL	
		ODV
THE	CITY OF NEW Y	UKN
	0 1	
	Appearance Card	
I intend to appear and	speak on Int. No.	Res. No
	in favor in appositi	272
	Date	1/20/23
N- Dice to	(PLEASE PRINT) Scott Semo	ne
1110	1	
Address:	D	
I represent:		
Address:		
to send the send of the send o		
The section of the	THE COUNCIL	The second secon
THE		ODK
IHL	CITY OF NEW Y	UNA
	Appearance Card	
L		
	peak on Int. No.	
	in favor in oppositio	1/20/23
	Date:	1/20/23
01,0	(PLEASE PRINT) Ruben Beltrun	1/20/23
Name: Chiet	Kuben Beltran	
Address: NYPD	>	
I represent:		
		The second secon
Address:		
		A



	7
Appearance Card	
I intend to appear and speak on Int. No Res. No	
in favor in opposition	
Date:	_
Name: PLEASE PRINT) OURS	_
Address: 11379	_ j#
I represent: FRELANCE	_
Address:	_
Please complete this card and return to the Sergeant-at-Arms	4
	MARKET COLUMN
THE COUNCIL THE CITY OF NEW YORK Appearance Card]
I intend to appear and speak on Int. No Res. No	
in favor in opposition	
Date:	_
(PLEASE PRINT)	
Name: HNIARCO	_
Address:	
I represent:	
No sala	
Address:	4
Please complete this card and return to the Sergeant-at-Arms	