



New York Media Consortium



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 real time. Encryption of all 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 real-time 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 qualified 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 no 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 receivers 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 not involve qualified journalists who have been listening to unencrypted communications on scanning receivers for years. Those instances involve the illegal use of a transmitter (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 real-time 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