MIAMIBEACH
POLICE

MEMORANDUM

TO: **Jimmy L. Morales**
City Manager

FROM: **Daniel J. Oates**
Chief of Police

DATE: **July 13, 2017**

SUBJECT: **Police Department Comment on Revised ACLU Surveillance Ordinance**

Introduction

This memorandum is prepared as an update to my original memorandum dated October 18, 2016. It reflects my revised comments based on the second version of the Surveillance Ordinance submitted by the American Civil Liberties Union (ACLU) on July 6, 2017. This memorandum is prepared in anticipation of likely discussion of this new version of the ordinance by the City Commission at its upcoming July 26 meeting.

Even in its revised form, if this proposed Ordinance is adopted, it will have a severe negative impact on the basic operations of the Miami Beach Police Department, particularly on detective investigations, and it will significantly hinder our officers' ability to fight crime and keep the city safe.

The proposed Ordinance will also severely handicap and perhaps prevent the Department from conducting many basic tasks we deem essential, such as: sharing information with colleague law enforcement agencies; using license plate readers or red light cameras; deploying and monitoring traffic cameras or speed trailers; using covert listening devices for the protection of undercover officers and for evidence collection; or using covert cameras for criminal investigations or in a crisis situation such as an active hostage scenario.

The Ordinance also places an extraordinarily excessive administrative burden on the Department. This includes requiring the Department to prepare a "Surveillance Impact Report" and a "Surveillance Use Policy" for each and every "surveillance technology," as that term is defined in the Ordinance, that the Department is currently using or new surveillance technology that the

Department desires to use in the future. The Ordinance also requires the Department to prepare a yearly "Annual Surveillance Report" for each surveillance technology the Department wishes to continue utilizing. Each "Annual Surveillance Report" has various components that require statistical documentation and analysis. This analysis must then be presented to the City Commission for a determination, based on the information provided by the Department in the "Annual Surveillance Report," as to whether the Commission will reauthorize the use of each such surveillance technology for the following year. These reporting requirements are so burdensome that many tasks and technologies we currently rely on – or had hoped to use in the future to advance our effectiveness – would likely have to be abandoned because the Department simply cannot afford to allocate the excessive staff time needed to justify new or continued use of these surveillance technologies.

The Miami Beach Police Department is fully accredited by the Commission for Accreditation of Law Enforcement Agencies (CALEA). As such, the Department is already among the top five percent (5%) of police agencies in the United States in terms of adherence to best practices in law enforcement. The Department has numerous policies that guide us on the broad issue of surveillance. All have passed muster with CALEA inspectors. Our policies cover the breadth of the topics and issues typical for a large, enlightened police organization, including areas such as: use of audio/visual surveillance equipment; narcotics and vice investigations; radio communications; organized crime, public corruption and terrorism investigations; intelligence gathering and the collection, storage and purging of intelligence information; deployment of license plate readers and red light cameras; and use of social media.

In my judgment, major reforms of these policies are unnecessary. I am not aware of any complaints on this subject in my three-plus years as police chief, and veteran command staff members cannot remember receiving any such complaints in the course of their entire careers. Furthermore, the Department utilizes its surveillance technology within the bounds of the law and obtains any legally required court orders, subpoenas or warrants for use of its surveillance technology or obtaining of surveillance data and does so with judicial approval and/or in conjunction with the Miami-Dade State Attorney's Office.

If the Commission is concerned about particular aspects of the Department's use of "surveillance technology," as broadly defined in the Ordinance, my recommendation is that the Commission considers an alternative approach. I suggest that the Department work with the Commission, through a designated policy committee, to do a comprehensive review of Department surveillance technologies currently in use, evaluate national best practices, and ask the Department to address any concerns the policy committee may have. In addition to adhering to Constitutional protections, the Department already scrupulously follows all budgeting and contracting/procurement rules when acquiring new equipment and new technologies. If Commissioners have individual concerns, it

may be possible to address them on a case-by-case basis and perhaps by simple policy changes rather than a sweeping Ordinance that has potential for a multitude of unintended, negative consequences.

In my experience, the policy discussions in this arena that have typically been of particular interest to elected officials and other policy makers have centered on a handful of narrow issues. These have typically concerned: 1) the length of time a police department retains images and data: 2) who has access to data collected: 3) when and under what circumstances records are shared with parties other than law enforcement; 4) and whether intelligence information on persons or groups are maintained, shared and/or purged in a manner that follows best national practices so as to ensure that there are no privacy or First Amendment violations. It may be helpful in any discussions with the Commission to focus first on these most common areas of concern, although we feel that the Department already has sensible rules on these issues in place.

Specific Concerns and Impacts of the Ordinance

One of the many reasons that crime has fallen so precipitously across America and in Miami Beach in the past three decades has been the smart use of evolving new technologies to fight crime. “Surveillance technologies,” as so broadly defined in the Ordinance, are critical tools in the police arsenal that enable our Department to keep our residents, visitors and employees safer. Tools such as license plate readers, interrogation room video recorders, crime analysis software, and fixed surveillance cameras that can monitor public areas for crime and traffic issues are vitally important to the Department. The proposed Ordinance is extremely broad in its definitions, the scope of its restrictions on the use of these and other “surveillance technologies,” and in the administrative burden placed on the Department.

While not a complete list, here are some specific concerns the Police Department has with the proposed Ordinance:

1. The Ordinance requires that every piece of surveillance technology, whose description, purpose and how it works will be contained within the “Surveillance Impact Report” and “Surveillance Use Policy,” be posted on the City’s website for all to see. Furthermore, to have public discussion for all to hear prior to the Department acquiring or using any new or current surveillance technology will severely hinder the Department’s ability to prevent criminal conduct and apprehend criminals. To post on the City’s public website, along with a public discussion of all the City’s surveillance technologies, will provide criminals with a roadmap of where and how to perpetrate any criminal conduct in a manner and location so that police are far less likely to detect it or capture the criminal. As just one example of how problematic this requirement is, consider the use of covert recording devices that an undercover officer might wear for his/her own

safety. What the device looks like and how it is hidden on the officer would have to be posted on the city's website, an absurdity for a device designed to keep the officer safe from detection of his/her undercover status.

2. The Ordinance is broadly drafted such that the term "surveillance technology" encompasses many police tools with limited exceptions for certain items such as computers, printers, televisions, radios, body worn cameras and binoculars. Such a broad definition will require the Department to request and obtain Commission approval before seeking funds, accepting funds, acquiring (even through donation), borrowing or utilizing most new or existing surveillance technology. Furthermore, the Ordinance requires the time-consuming preparation of the previously-mentioned Surveillance Impact Report, which must include, among other things, a description of the technology, how it works, the purpose of the technology, and the data that the surveillance technology is capable of collecting, capturing, recording, intercepting or retaining. Additionally, it is important to recall that all of this information must be posted, un-redacted, on the City's website for all to view for the entire duration that each surveillance technology is in use. As just one example of how problematic this requirement is, consider the use of covert fixed cameras used for ongoing surveillance in a criminal investigation. If made public on the city's website, not only would the cameras be rendered useless, but the criminal targets would immediately learn they are under investigation.

3. The Ordinance requires a "Surveillance Use Policy" for any new or existing surveillance technology. The policy must address, among many other things, the specific permitted use(s) and purpose(s) of the surveillance technology, including the places, times, manner and circumstances under which each surveillance technology may be used, including any limitations on the crimes that may be investigated with it. Additionally, the Surveillance Use Policy must include a "Public Access" component addressing how the public may access the surveillance data and what steps will be taken to protect individual privacy. These underlined sections make clear that any surveillance done by the Department for any law enforcement purpose will be completely public information and totally accessible, rendering worthless and counterproductive any effort of the Department to use surveillance technology on an active criminal investigation, an internal affairs investigation, an employee misconduct investigation for another city agency, etc. In addition, there are other requirements within the Surveillance Use Policy section that are overly burdensome to the Department.

4. Upon obtaining approval for the use of a surveillance technology, the Ordinance requires that an "Annual Surveillance Report" be prepared and

submitted to the City Commission. The Ordinance only allows, unless explicitly stated otherwise, each surveillance technology to be utilized for a period of one (1) year before the Commission must annually review and reauthorize the technology anew based on the "Annual Surveillance Report." This report must also be publicly posted in an unredacted form on the City's website and handed out as a public record to anyone who requests it. As an example of how problematic this requirement is, consider that a robbery or theft suspect could use this information to determine, in advance, where he/she could most likely victimize someone on the street without getting caught by simply having knowledge of where the Department has its street-monitoring cameras located.

5. The Ordinance also declares that any funding, acquisition or utilization of surveillance technology that has not been approved pursuant to the Ordinance, or the use of surveillance technology in a manner or for a purpose that has not been approved pursuant to the Ordinance, constitutes an injury, and that any person may then institute a lawsuit and such plaintiff can potentially recover costs and attorneys' fees in addition to obtaining injunctive or declaratory relief and suppression of any evidence obtained from the use of such surveillance technology. So with this Ordinance, the City would effectively be inviting itself to be a target as a defendant in a new arena of civil litigation, with the potential for liability for even the most common police practices. This would eventually, over time, result in the Department curtailing crime-fighting practices to avoid risk. Also, we should expect union opposition to this Ordinance because of the additional unnecessary exposure that it will place on individual officers as potential defendants in these same civil lawsuits. While opposition by a labor group to an innovation in policing is not necessarily a reason to forego the change, in this case I believe these concerns about increased liability would have real merit.

6. The Ordinance requires a huge allocation of police personnel and monetary resources to comply with its administrative mandates. The compilation and analysis of the data for each surveillance technology, along with preparing a "Surveillance Impact Report," a "Surveillance Use Policy," and/or an "Annual Surveillance Report" would be an overwhelming and unattainable burden. In my opinion, it is inevitable that with these kinds of reporting requirements, the Department will eventually simply stop using much of the technology we already use to fight crime.

7. The Ordinance has an all-encompassing public records disclosure requirement. The "Surveillance Impact Report", the "Surveillance Use Policy" and the "Annual Surveillance Report" are to be posted online on the City's webpage and provided to the public without redaction. Upon request, or by merely going to the City's website, anyone would be able to obtain complete information and details regarding each and every

surveillance technology at the Department's disposal. Furthermore, the Ordinance requires that the public be instructed on how to access the data captured by any surveillance technology and also requires the City to take steps to protect individual privacy in allowing the public access to such surveillance technology data. An undetermined amount of additional civilian staff would have to be added to the Department's Records Unit to deal with these requests.

8. The Ordinance also requires the Surveillance Use Policy to address what procedures will be put in place so that members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific surveillance technology, and what internal personnel will be assigned to receive, register, track and respond to such communications. This essentially requires the Department to maintain a perpetual question-and-answer desk for anyone to ask, complain or question anything he/she would like regarding the City's deployment or usage of any surveillance technology. An undetermined amount of additional civilian staff would have to be added to the Department to deal with these inquiries.

9. The Ordinance is less than clear on what the full obligations are of the MBPD when it shares the results of surveillance technology with other agencies, as well as when it accepts such data from another agency that has used surveillance technology. The MBPD routinely shares such information with colleague law enforcement agencies in order to reduce crime. More analysis would need to be done to determine how the Ordinance impacts such routine and common practices between the MBPD and its partners as the sharing of photos, intelligence, forensic material and records information with our local, state and federal partners.

Conclusion

The ACLU's revised Surveillance Technology Ordinance is still unacceptable in my view as Police Chief. It will severely impact the Police Department's ability to perform basic crime-fighting efforts and to use technology smartly to do so. It will also impact basic operations such as the use of surveillance cameras and photo red light cameras. It will expose the Department and the City to new levels of civil liability and unintended consequences. It will potentially increase the exposure of police officers and the City to lawsuits. We can expect that it will be opposed by our police officers' labor union, and this likely opposition has merit.

I am aware that major city police departments have dealt with surveillance and privacy issues in the past 30 years, but these have typically been much larger police agencies and cities than Miami Beach. I am aware of issues over the years in New York, Los Angeles, Chicago and Denver, for example. In these cities, the public debate, policy setting and/or First Amendment litigation

generally focused on four areas of reform or guidance: 1) the length of time a police department retains images and data: 2) who has access to data collected: 3) when and under what circumstances records are shared with parties other than law enforcement; and 4) whether intelligence information on persons or groups are maintained, shared and/or purged in a manner that follows best national practices. These are all areas in which the MBPD currently has reasonable policies in place that meet CALEA standards.

I still believe that a better course of action on this topic would start with a dialogue between the Commission, the ACLU, the Department and any other potential stakeholders about what, if any, perceived harm this Ordinance is attempting to correct. Is there really a need for a change in any MBPD practices or policies? If, in fact, the Commission determines a need for policy changes regarding MBPD's use of surveillance technology, these changes almost certainly could be accomplished through more modest and simple amendments to existing Department policy rather than through a sweeping new city ordinance that is detrimental to police operations.