Minneapolis
City of Lakes

# Police Conduct Oversight Commission

# Surveillance Whitepaper

March 2019

# Contents

## Executive Summary

The Minneapolis Police Department (MPD) deploys basic surveillance tools throughout the city of Minneapolis. Video recording devices include public safety cameras, body worn cameras, and mobile video recorders (squad cameras). All devices require manual operation, and no analytical software automates recognition of those captured in recordings. The software interface for public safety cameras allows them to operate as a closed-circuit television system with recordings saved for 14 days. Additional software functions as a mailing list for privately-owned cameras, allowing police to easily request copies of potential recordings.

The Minneapolis Police department does deploy two pieces of automated technology, Shotspotter and automated license plate readers. Neither links images of individuals to personal information. License plate readers automatically match plates with law enforcement databases.

It is worth noting that law enforcement agencies other than the Minneapolis Police Department have deployed various advanced surveillance technologies within the City of Minneapolis. While the PCOC has no jurisdiction over these agencies, information or equipment sharing with the Minneapolis Police Department could be a subject for further review. This may occur outside of PCOC.

Finally, surveillance technology is developing at a rapid rate, and vendors used by the Minneapolis Police Department (such as Axon) are working on automated solutions. While the Minneapolis Police Department has no current plans to incorporate these into its existing systems, it is conceivable that this could change in the near future. Exploration of the cost of such technologies may be warranted as this would determine who would be alerted to their acquisition.

## 1. Introduction

During the June 12, 2018 Police Conduct Oversight Commission Meeting (PCOC), Council Member Steve Fletcher approached the PCOC with a request for information regarding the current state of surveillance technology in Minneapolis. The PCOC moved to conduct an initial exploration of the subject with the general goals of answering:

1. What data is MPD gathering from surveillance technology?
2. How is MPD storing the data?
3. How long is MPD are storing the data?
4. Who is allowed access to the data?
5. Who initially decides what data MPD collects?

This whitepaper will attempt to answer these questions in a concise format. Research for the paper involved interviews with employees of the Minneapolis Police Department (MPD) and Downtown Improvement District, review of publicly available investigative reports that involved surveillance technology, review of software used by MPD, and review of city contracts. Analysts did not review or audit of the actual surveillance data as it was not within the scope of the project.

## 2. Public Safety Cameras

Public safety cameras exist in all precincts, with each precinct responsible for its own camera monitoring and maintenance. The cameras record video which is maintained on city owned servers for 14 days after which it is permanently deleted. Video captured within the 14 day period can be reviewed using Milestone Software from Arxys which manages all the cameras and links them to the recording server.

Recordings can be retained if there is a reason to do so, such as when a crime is captured on video. When this occurs, the video is transferred from the server to another "legally acceptable medium." Retention of these videos follow a separate schedule linked to the related criminal investigation. The MPD controls access to recordings in conformance with the Minnesota Government Data Practices Act.

Verizon provided additional cameras prior to the Super Bowl, and these are still in operation. They were integrated into the Milestone system and function similarly to the preexisting cameras. MPD placed them in downtown areas relevant to Super Bowl traffic.

Precinct 1 (downtown) is unique in that the Downtown Improvement District (DID) partners with the MPD to provide more cameras, civilian monitoring, and communication with social service providers. The DID, a 501(c)6 non-profit, provides a variety of services downtown and is supported by its ordinance allowing higher taxes paid by commercial property owners in the

district. MPD owns the data created by DID's cameras and stores and maintains it like all other public safety camera recordings.

Employees of DID who monitor cameras go through background processing like an MPD officer, are interviewed by a lieutenant in the MPD Business Technology unit, and function similarly to a security vendor. They have access to the cameras within the special district. They are connected via a radio channel to social services but not directly to MPD. According to DID, they use 911 to report crimes they witness on camera.

DID assisted MPD in developing a CCTV Policy found in Appendix 1. All employees accessing the camera system are required to read and initial each page of the policy. The final section is noteworthy in that it establishes "compliance officers" responsible for regularly auditing the system to ensure proper use and functionality. MPD has designated a supervisor from each precinct to serve as the compliance officer. The policy does not dictate metrics for audit.

MPD's CCTV system does not use any automated technology (such as facial recognition) to analyze real-time video. The system requires manual operation of all public safety cameras, and no one interviewed for this whitepaper expressed any interest in adding this functionality at this time.

## 3. Securonet

Securonet sells a variety of surveillance related technologies, namely Safelink, Videolink, and Fieldwatch. MPD currently uses Safelink to bolster the CCTV system. MPD can enter location information into the system, and Safelink will show on a map any registered privately-owned camera in the area. MPD can then contact the owner and request a copy of the recording. Camera owners must register their cameras to be listed, and Safelink does not provide MPD access to privately owned camera feeds. No data other than the list of users is stored using this system.

Videolink takes this a step further and allows law enforcement to livestream from privately-owned cameras. The owner must grant permission to law enforcement to stream. According to command staff, MPD does not currently use Videolink. The website advertising the product uses a photo of MPD officers as the header, which caused some confusion.

Fieldwatch was used by MPD during the Super Bowl and other large-scale events. It allows cell phones running the Fieldwatch app to provide location data and stream video. While MPD employs body cameras for field recording, Fieldwatch can act as a supplement for those not assigned a BWC and provides streaming video to command staff (current BWCs do not have this capability). Recorded video can be downloaded from Securonet's program and added to evidence.com to comply with retention policies, the current platform for storing body camera recordings.

## 4. BWCs and MVRs

MPD's use of body worn cameras has been reviewed by Internal Audit and quarterly reports are issued by MPD's Quality Assurance Unit. This whitepaper will not review the results of the prior audits or the body camera recording retention policy. MPD staff confirmed that MPD is not currently employing software analytics (such as facial recognition) with BWC video nor technology that would allow livestreaming of BWC feeds. The manufacturer of MPD's body worn cameras is developing automated solutions.

## 5. Automated Technology

MPD currently uses several pieces of automated surveillance technology, Shotspotter and Automated License Plate Readers (LPRs). Shotspotter uses audio sensors and software to detect gunshots. If a gunshot is detected, it alerts law enforcement. Shotspotter records audio before and after an incident classified as a gunshot, and audio is not livestreamed. Questions have been raised about whether Shotspotter records more than just potential gunshots, as audio recordings of speech captured by Shotspotter have been used as evidence in criminal trials.

LPRs take photographs of vehicles and uses software to automatically match license plates to law enforcement databases. Minnesota Statute 13.824 governs the use of LPRs by any agency and requires a biennial audit by an independent agency of records, use, and compliance with retention requirements (an example of which can be found here). Data obtained via LPRs is destroyed within 60 days of the date of collection unless it is related to an active investigation.

Sharing LPR data across agencies raises concerns, as this data provides information about a subject's movement and frequented destinations. To share data with another law enforcement agency, the chief (or the chief's designee) must provide written authorization and document the specific legitimate law enforcement purpose for sharing the data. Sharing may only occur if the data pertains to an active criminal investigation. As documentation of the request is required, PCOC could request access to current sharing agreements if an audit were conducted.

## 6. Non-MPD Technology Deployed in Minneapolis

While not technically within the scope of this report, it is worth noting that the multitude of law enforcement agencies operating within Minneapolis may use advanced surveillance technology within the city. For example, during the investigation of the shooting of Jamar Clark, BCA investigators used a cell-site simulator, commonly known as a Stingray or KingFisher, to locate a potential witness in Minneapolis. These devices create simulated cell towers in an attempt to locate a specific phone that inadvertently connects to it. It appears that Hennepin County also owned a similar device at one point in time, but they have since stated that they discontinued using the device.