

March 25, 2021

To: Fire and Police Commissioners and Executive Director
From: Paul Mozina
Re: FPC21056 Standard Operating Instruction SENSITIVE CRIMES
DIVISION

I am concerned that the MPD's addition of paragraph G., under section IV. RESPONSIBILITIES, is vaguely worded and does not adequately and explicitly account for digital file systems, database, and applications via which the MPD electronically stores information related to sensitive crimes.

Here is what paragraph G. says:

The SCD shall ensure that all evidence related to investigations is collected and inventoried pursuant to department policies. SCD members shall ensure that any media storage device(s) or printed document(s), to include any working copies, are protected from public view and properly secured in a locked area by the member responsible for the media storage device(s) or printed document(s).

There is no mention of protecting the Investigative File, or any of the other documentation and evidence associated with the case from MPD members who do not have a legitimate and approved need to see the information. The problem with the leaking in December 2018 of Jane Doe's investigatory file and the video interview with the alleged suspect was not that the information was not protected from public view, it was not protected from unauthorized view by MPD members, which makes it virtually impossible to secure the information.

Jane Doe's case highlights the importance of protecting the information, IN ALL FORMATS physical and digital, related to sensitive crimes investigations.

Under Section 4, paragraph a. in Jane Doe's Settlement Agreement with the MPD it says:

- a. MPD Sensitive Crimes Division (SCD) shall implement a secure file storage system that protects and maintains the privacy rights of reporting victims. All files, case records, and evidence shall be stored in locked cabinets to which only SCD detectives and supervisors will have keys. Anyone else seeking access must request permission and a record shall be maintained of anyone requesting files and/or evidence and the purpose of their request.

March 25, 2021

And even here, a reference is made to “locked cabinets” rather than digital file systems, databases and applications. But when we examine the Witness Statements made to Mr. Mel Johnson during his investigation of the leak, we see many references to investigative reports and video that are stored online. Sensitive Crimes Division Captain John Corbett simply decided to make another copy of the video interview in addition the 4 normally made and gave it to Gulbrandson. Not satisfied with this, Gulbrandson access the video archive system directly and download another copy of the video without asking for authorization of form Inspector Terrence Gordon, who was in command of the SCD at the time.

Information related to ongoing investigations is stored in a myriad of places including:

- The Automated Reporting System (ARS)
- The Domestic Violence Supplement Incident Report (form PO-15D)
- The DA Sheets and DA Charging Packet
- The Charging Conference Supplemental Report
- The Domestic Violence Misdemeanor Suspect Want (form PD-36)
- The Case Track System
- The Investigative Reports

It is imperative that the SOI SENSITIVE CRIMES DIVISION be updated to explicitly address digital secure file systems, including those for video, and secure them from unauthorized access by MPD members AND the Public.

Sincerely,

Paul Mozina