Councilmember David Grosso

AN AMENDMENT

#1

Date: July 7, 2020

Amendment offered by: Councilmember David Grosso

To: Comprehensive Policing and Justice Reform Second Emergency Amendment Act of 2020

Version:

Introduced	_____
Committee Print	_____
First Reading	X
Amended First Reading	_____
Engrossed	_____
Enrolled	_____
Unidentified	_____

Amendment:

A new subtitle is added to read as follows:

SUBTITLE __. LIMTS ON BIOMETRIC SURVEILLANCE

Sec. ___. The Metropolitan Police Department Video Surveillance Regulations Act of 2002, effective October 1, 2002 (D.C. Law 14-190; D.C. Official Code § 5–133.19), is amended by adding new sections 2701a and 2701b to read as follows:

"Sec. 2701a. Definitions.

"For the purposes of this subtitle, the term:

"(1) "Biometric surveillance system" means any computer software that performs facial recognition or other remote biometric recognition in real time or on a recording or photograph.

"(2) "Facial recognition" means an automated or semi-automated process that:

"(A) Assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating surveillance information about an individual based on the physical characteristics of the individual's face; or

"(B) Logs characteristics of an individual's face, head, or body to infer emotion, associations, activities, or the location of an individual.

"(3) "Other remote biometric recognition" means an automated or semi-automated process, not including identification based on fingerprints or palm prints, that:

"(A) Assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating surveillance information about an individual based on the immutable characteristics of the individual ascertained from a distance, such as gait;

"(B) Uses voice recognition technology; or

"(C) Logs immutable characteristics, such as an individual's gait, to infer emotion, associations, activities, or the location of an individual.

"(4) "Voice recognition technology" means the automated or semi-automated process that assists in identifying or verifying an individual based on the characteristics of an individual's voice.

"Sec. 2701b. Limits on use of biometric surveillance.

"(a) It shall be unlawful for any District law enforcement agency, agent, or official to acquire, possess, access, or use:

"(1) Any biometric surveillance system; or

"(2) Information derived from a biometric surveillance system operated by another entity.

"(b) Nothing in subsection (a) shall prohibit the District or any District official from:

"(1) Obtaining or possessing an electronic device, such as a cell phone, tablet, or computer, that performs facial recognition or other biometric recognition for the sole purpose of user authentication; or

"(2) Using facial recognition or other biometric recognition on an electronic device, such as a cell phone, tablet, or computer, owned by the District or any District official, for the sole purpose of user authentication.".

Rationale:

This amendment would limit the use of facial recognition and other biometric recognition surveillance by MPD and other D.C. law enforcement agencies. These technologies are very new and associated with inaccuracies based on race in particular but also gender and other characteristics. The first cases of false arrest using these technologies are emerging and unsurprisingly Black people bear the brunt of these violations. The amendment would not prevent anyone from having or using devices that use biometric recognition, such as finger-print or face identification, to unlock a phone. Further, the amendment would not change the status quo with regards to fingerprint and palm-print technology.

Councilmember David Grosso

AN AMENDMENT

#2

Date: July 7, 2020

Amendment offered by: Councilmember David Grosso

To: Comprehensive Policing and Justice Reform Second Emergency Amendment Act of 2020

Version:

Introduced	_____
Committee Print	_____
First Reading	X
Amended First Reading	_____
Engrossed	_____
Enrolled	_____
Unidentified	_____

Amendment:

A new subtitle is added to read as follows:

SUBTITLE __. LIMTS ON CELL-SITE SIMULATOR TECHNOLOGY

Sec. ___. (a) It shall be unlawful for any District law enforcement agency, agent, or official to acquire, possess, access, or use cell-site simulator technology.

(b) For the purposes of this section, the term:

(1) "Cell-site simulator technology" means software or hardware that transmits or receives radio waves while simulating an electronic communications device or cellular phone tower, site, or service. The term includes international mobile subscriber identity catchers or other surveillance or eavesdropping devices that mimic cellular phone towers and send out signals to do one or more of the following:

(A) Identify, locate, or track the movements of a communications device;

(B) Intercept, obtain, access, or forward the communications, stored data, or metadata of a communications device;

(C) Affect the hardware or software operations or functions of a communications device;

(D) Force transmissions from or connections to a communications device; or

(E) Deny a communications device access to other communications devices, communications protocols, or services.

(2) "Communications device" means a cellular telephone, tablet, laptop, hot spot, or other hardware that enables transmission of electronic communications, or enables access to an electronic communications system, electronic communication service, remote computing service, or geolocation information service.

Rationale:

This amendment would prohibit the use of cell-site simulator technology by MPD and other D.C. law enforcement agencies. One popular brand is called Stringray. Originally developed by the military, these technologies are extremely invasive into individuals' privacy, capturing wide swaths of personal data by taking advantage of the ubiquity of cell phones in modern society. The technology mimics a cell phone tower, tricking a cell phone into transmitting information to the technology. This technology gathers personal data ranging from metadata such as numbers called and location of the cell phone to the actual content of texts and sometimes prevent messages or calls from going through to their actual intended target. The secretive nature of these technologies and their invasion into our privacy warrants strong limits on their use, at least for the time being. This is one step in demilitarizing the police.