Sec. 10-63. Exceptions and exemptions.

(a) For the purposes of this article, the following do not constitute surveillance data or surveillance technology, and the requirements of this article do not apply to them:

(1) Surveillance data acquired where the individual knowingly and voluntarily consented to provide the information, such as submitting personal information for the receipt of city services; and

(2) Surveillance data acquired where the individual was presented with a clear and conspicuous opportunity to opt out of providing the information.

(b) For the purposes of this article, surveillance technology and surveillance data do not include the following devices, software, or hardware and are exempt from the requirements of this article, unless the devices, hardware, or software are modified to include additional surveillance capabilities as defined in section 10-62:

(1) Routine office hardware, such as televisions, computers, and printers, that are in widespread public use and will not be used for any surveillance or surveillance-related functions;

(2) Parking ticket devices (PTDs) and related databases.

(3) Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is used for manually capturing and manually downloading video and/or audio recordings;

~~(4) Body-worn cameras;~~

(4) Cameras installed in or on a police vehicle;

(5) Cameras installed pursuant to state law authorization in or on any vehicle or along a public right-of-way solely to record traffic violations or traffic patterns, provided that the surveillance data gathered is used only for that purpose;

(6) Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;

(7) City databases that do not and will not contain any surveillance data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology;

(8) Manually-operated technological devices that are used primarily for internal city communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;

(9) Parking access and revenue control systems, including proximity card readers and transponder readers at city-owned or controlled parking garages;

(10) Card readers and key fobs used by city employees and other authorized persons for access to city-owned or controlled buildings and property;

(11) Cameras installed on city property solely for security purposes, including closed circuit television cameras installed by the city to monitor entryways and outdoor areas of city-owned or controlled buildings and property for the purpose of controlling access, maintaining the safety of city employees and visitors to city buildings, and protecting city property;

(12) Security cameras including closed circuit television cameras installed by the city to monitor cashiers' windows and other cash-handling operations and to maintain the safety of city employees and visitors to such areas;

(13) Cameras installed solely to protect the physical integrity of city infrastructure; or

(14) Technology that monitors only city employees in response to complaints of wrongdoing or in order to prevent waste, fraud, or abuse of city resources.

(Ord. No. 2019-20 , 10-10-2019; Ord. No. 2021-01 , 2-25-2021)