

MEMORANDUM
Office of the City Attorney



Disclosable Public Record

Date: November 17, 2011
To: Mayor Esteves and Members of the City Council
From: Michael Ogaz, City Attorney
Subject: **Public Records**

Issue

Are security videos and records of security key card usage disclosable public records?

Short Answer

Security video footage and records of security key card usage are public records, but are protected from disclosure pursuant to Government Code Section 6254(f) as security files compiled for law enforcement purposes.

Analysis

The California Public Records Act (Gov. Code, § 6250 *et seq.*; hereafter CPRA) authorizes “access to information concerning the conduct of the people’s business is a fundamental and necessary right of every person in this state.” Gov. Code § 6250. To implement that right, the Act declares that “[p]ublic records are open to inspection.” Gov. Code § 6253. At the same time, the Act recognizes that certain records should not, for reasons of privacy, safety, and efficient governmental operation, be made public. *See Haynie v. Superior Court* (2001) 26 Cal.4th 1061, 1064 (“*Haynie*”). While reference is made to protection of privacy rights, the CPRA provides little in the way of actual protection except regarding personnel and medical records. Gov. Code § 6254(c). Nonetheless, the California State Constitution protects its citizens’ right to privacy and from disclosure that might violate a particular person’s privacy rights, depending on the circumstances.

Govt. Code §6254(f) authorizes a public agency to withhold “[r]ecords of complaints to, or investigations conducted by, or records of intelligence information or security procedures of, the office of the Attorney General and the Department of Justice, and any state or local police agency, or any investigatory or security files compiled by any other state or local police agency, or any investigatory or security files compiled by any other state or local agency for correctional, law enforcement, or licensing purposes...” The CPRA exempts these records from disclosure, although it does require the agency to disclose certain information derived from them. *Williams v. Superior Court* (1993) 5 Cal.4th 337, 353 (“*Williams*”).

Several cases have analyzed whether or not certain documents are part of an investigatory file and when the investigatory file becomes protected from disclosure. *See Haynie and Williams, supra*. The courts have required that for investigatory files to be withheld from disclosure there must be a concrete and definite prospect of a criminal law enforcement proceeding. *See Uribe v. Howie* (1971) 19 Cal.App.3d 194, 212-13. “To say that the exemption created by subdivision (f) is applicable to any document which a public agency might, under any circumstances, use in the course of [an investigation] would be to create a virtual *carte blanche* for the denial of public access to public records. The exception would thus swallow the rule.” *Id.*

Although case law has provided clear parameters with regard to investigative files, we have been unable to find such requirements for the non-disclosure of security files. Arguably, the concern of the exception swallowing the rule is likely not applicable to security files. Whereas an investigatory file could contain policies, procedures, memos, interviews, reports and other documents related to an investigation, these security files are only a monitoring of events retained for the safety of public facilities and personnel. Consequently, it is unlikely that a court would require a showing of whether criminal prosecution is likely, as they do for investigative files.

The City’s video surveillance and records of security key card usage are security files since the primary reason for obtaining the information is to record events for security and law enforcement purposes. We have consulted with Information Services Director Bill Marion about the genesis of these security devices. As Mr. Marion explains, the video cameras at City Hall were put in place in response to the 9-11 catastrophe and were intended primarily to prevent criminal activities. The cameras are set up in areas, such as entrances to public buildings or in the garage, where criminal activity might occur. The security key card records have been used to track access to secure areas, such as the cashier’s cage, to be used in the event of theft or misappropriation. Their primary purpose, therefore, is for building security. Consequently, a court is likely to find that the video surveillance and security key card usage records are security files exempt from public disclosure under Section 6254(f).

As previously noted, we find no case law contradicting this interpretation of Section 6254(f). On the other hand, we find no cases that specifically hold that such videos or key card information are “security files” exempt from disclosure under the Public Records Act. Most of the cases reviewing security information have employed a balancing test to determine whether the public interest in disclosure outweighs the public interest in nondisclosure. However, the City of Milpitas is prohibited from using this balancing test pursuant to the Open Government Ordinance, Milpitas Municipal Code Section I-310-3.70(g). Nonetheless, we opine that a specific exemption exists from the CPRA disclosure requirements based on the conclusion that these records are security files compiled by the City of Milpitas for law enforcement purposes, within the meaning of Government Code Section 6254(f).

The opinion set forth herein applies only to the video surveillance cameras at City Hall, the entrance gate at the corporation yard and those located at the sewage pump station, and to all security key card entry data citywide. These devices were all clearly installed for the primary purpose of law enforcement security. Other videos, for instance those installed for traffic management purposes, may not fall within this exemption.