Cyber-Resilience Considerations & Inputs on Council Item: Amending BMC 2.99 to Prohibit City Use of Face Recognition Technology	Date: 06/24/2019

Attendant Questions

1) Is there any impact on the definitions of 2.99.020?

WHY ASKED: Apple FaceID is perhaps the best known use of Face Recognition Technology for Cybersecurity.
Cybersecurity capabilities include the use of Face Recognition Technology as part of:

a. Identity verification (e.g., during account set up)
b. Account use (at log-in)
c. Preventing fraud

The face is one of a number of "data points" used in cybersecurity to reduce the risk of someone besides you misusing your (a & c) personal information and (b) your account.
FIDO Alliance is working on linking Face Recognition Technology with Blockchain Technology to increase the privacy and return of ownership of personal information and accounts to the individual.
Prohibiting Face Recognition Technology in this case would dictate a lesser level of privacy within the City's uses.

END RESULT:

- If there is an impact, then: BPD's and the City's use of Apple FaceID (and other Face Recognition Technology for cybersecurity) is prohibited by this proposal.
- If there is no impact, then the City can continue to use Apple FaceID and other/future Face Recognition Technology for cybersecurity.

2) Which Face Recognition Technology is being prohibited?

WHY ASKED: There are three (3) categories and the City already uses one in its Park CCTV for San Pablo Park.

The 3 categories are:

- Biometric AI (artificial Intelligence) – face pattern recognition
- Non-invasive Iris Scan
- Behavioral AI – gait analysis, lip reading, voice recognition.

The latter is used by the CCTV for San Pablo Park. This CCTV system may also use Biometric AI.

END RESULT: This amendment could prohibit the current system, increasing the immediate and long-term direct and indirect expense to the City while also reducing (at least momentarily) the safety of the park.

3) Given the adoption of Face Recognition Technology for the safety of their fire and police officers, would this prohibition become "fruit of the poisonous tree" within legal (and civil) cases involving the City of Berkeley?

WHY ASKED: Other jurisdictions are adopting Face Recognition Technologies as a means of reducing the insurance costs for their public safety officers. Typically the source of data is not captured during transmission. Instead, data sharing agreements/schedules are

	identified ahead of time and data controls are applied in the transmission to ensure only acceptable information is sent between organizations. The City is currently working on its draft Data Security standard. **END RESULT:** The use of Face Recognition Technology by another police department to identify a vehicle's driver (as compared to their owner) could make the unwitting use of such information by Berkeley Police Department (BPD) liable for a data point they had no control over, reducing the public safety efficiency and effectiveness of the Department. Similarly, not using such available technology could make the City liable for not ensuring everyone got out of a burning building. So this prohibition could also lead the City to higher one-time and ongoing personnel and operating expenses at some juncture, especially after litigation (by a Fire/BPD officer, by a community member, etc.). As an alternative, the Council should support City staff in completing and adopting a Data Security standard that includes data sharing restrictions effecting the City's values.
Recommendations:	1. Do not impede cybersecurity capabilities 2. Exempt the CCTV Face Recognition Technology used by the San Pablo Park CCTV 3. Support City staff in completing and adopting a Data Security standard
Drafted By	Tom Ray, Information Security Manager