ORDINANCE NO. _____

BILL NO. 112 (2026)

A BILL FOR AN ORDINANCE ESTABLISHING CHAPTER 8.37, MAUI COUNTY CODE, ON FACIAL RECOGNITION TECHNOLOGY

BE IT ORDAINED BY THE PEOPLE OF THE COUNTY OF MAUI:

SECTION 1. This Ordinance's purpose is to require that facial recognition technology used by a County law enforcement agency be used only in connection with a documented criminal investigation, with limited access to training and designated personnel, and require that a result generated by the technology be treated as an investigative lead rather than as proof of identity.

SECTION 2. Chapter 8.37, Maui County Code, is added to read as follows:

"Chapter 8.37

FACIAL RECOGNITION TECHNOLOGY

Sections:

8.37.010 Definitions.
8.37.020 Authorized uses; documentation required.
8.37.030 Limitations on use.
8.37.040 Access limitations.
8.37.050 Training.
8.37.060 Audit and accountability.
8.37.070 Construction.
8.37.080 Implementation.

8.37.010 Definitions. As used in this chapter, unless the context otherwise requires:

"Facial recognition technology" means an automated or semi-automated process that analyzes facial features in a photograph, video, or other image using a computer algorithm for the purpose of

identifying or verifying the identity of an individual, including comparison of an image against one or more databases of images. Facial recognition technology does not include:

1. Visual comparison of images by a person without the use of an identification algorithm;

2. Automated redaction of images for privacy purposes;

3. A feature used solely to authenticate the assigned user of a County-issued device or account; or

4. Automated license plate recognition.

"Criminal nexus" means articulable facts connecting the proposed use of facial recognition technology to a specific criminal offense that:

1. Has been committed, is being committed, or is being planned; and

2. Is the subject of a department case number or another law enforcement agency report number.

"Designated user" means an employee authorized in writing by the chief of police to access facial recognition technology.

"Immigration enforcement" means the same as defined in Act 141, Session Laws of Hawai'i 2026.

8.37.020 Authorized uses; documentation required. A. A county law-enforcement agency must not use facial recognition technology unless a criminal nexus exists and is documented before the technology is used.

B. Before each use, the designated user must record:

1. The department case number or another law enforcement agency report number;

2. A written statement of the criminal offense under investigation and the use's investigative purpose; and

3. An affirmation that the use for a criminal investigative purpose is consistent with this chapter and applicable department policy.

C. Where the entries required by subsection B can be recorded within the system used, they must be recorded within that system. Otherwise, they must be recorded in a log maintained by the agency.

D. Facial recognition technology may also be used, with the documentation required by subsection B adapted to the matter, and associated with a department case number or another law enforcement agency report number to:

1. Identify a deceased person;

2. Identify a person who is incapacitated or otherwise unable to provide identification; or

3. Locate a missing or endangered person.

E. Facial recognition technology may be used without prior documentation where there is an imminent threat of death or serious bodily injury to a person. The documentation required by subsection B, together with a description of the circumstances constituting the imminent threat, must be completed within 24 hours after the use.

8.37.030 Limitations on use. A. A result generated by facial recognition technology is an investigative lead and is not an identification.

B. A result generated by facial recognition technology, standing alone, does not establish probable cause, and must not serve as the sole basis for an arrest, a search, or an application for a search warrant. Probable cause must be established through independent investigation.

C. A result generated by facial recognition technology may be considered as one factor among the totality of the circumstances in determining whether reasonable suspicion exists to conduct an investigative detention if:

1. The result has been reviewed and confirmed by a designated user trained in facial comparison; and
2. At least one independent fact developed through investigation corroborates the result.

An unconfirmed or uncorroborated candidate result does not supply reasonable suspicion.

D. Nothing in this section limits the authority of an officer to conduct an investigative detention, to make an arrest, or to take other lawful enforcement action where reasonable suspicion or probable cause is established independent of facial recognition technology.

E. Facial recognition technology must not be used to identify or monitor an individual based on race, ethnicity, national origin, immigration status, religion, sex, gender identity, sexual orientation, disability, or other protected characteristic.

F. Facial recognition technology must not be used to identify or monitor individuals engaged in lawful assembly, protest, worship, political activity, or other activity protected by the first amendment to the United States Constitution or article I, section 4 of the Constitution of the State of Hawai'i, unless a criminal nexus exists that is independent of the protected activity.

G. Consistent with Act 141, Session Laws of Hawai'i 2026, facial recognition technology must not be used for the purpose of immigration enforcement, and a result generated by the technology may not be provided to a federal immigration authority for that purpose.

H. Facial recognition technology must not be used for the enforcement of civil traffic infractions.

I. Facial recognition technology may be deployed on a live camera only where the camera is directed at a public street, sidewalk, right of way, parking area, or other location open to public view or at a publicly-accessible area of premises open to the public and not directed into the interior of a private dwelling or lodging unit or into an area in which a person has a reasonable expectation of privacy, including a restroom or changing area.

8.37.040 Access limitations. A. Access to facial recognition technology is limited to designated users.

B. Each designated user must be granted the lowest level of system privilege needed to perform the user's assigned function. Where the system permits, access levels must be enforced technically and not by policy alone.

C. The chief of police must maintain a current written list of designated users and must review the list at least every three months.

D. Access must be terminated upon transfer, separation, or a determination that the employee no longer requires access.

8.37.050 Training. A. No employee may be granted access to facial recognition technology before completing department-approved training. Training must be documented.

B. Training must address the following:

1. The capabilities and limitations of the technology, including the potential for error and for differing rates of error across demographic groups;

2. The criminal nexus and documentation requirements of section 3;

3. The limitations in section 4, including the reliability and corroboration requirements, and the standards for reasonable suspicion and probable cause;

4. Constitutional protections applicable to the use of identification technology;

5. Applicable federal, state, and county law, including chapter 92F, Hawai'i Revised Statutes, Act 141, Session Laws of Hawai'i 2026, and 28 C.F.R. Part 23; and

6. Audit, misuse, and discipline provisions.

C. Refresher training must be completed annually.

8.37.060 Audit and accountability. A. Each use of facial recognition technology must be logged. The log must record the identity of the user, the date and time of the query, the case or report number, and the stated investigative purpose.

B. Logs must be retained for at least two years.

C. The chief of police must audit facial recognition technology use at least every three months for compliance with this chapter.

D. Use of facial recognition technology for a purpose other than one authorized by this chapter is prohibited. Violation of this chapter must be addressed under applicable policies governing employee conduct, including discipline that may include termination, and may be referred for criminal prosecution where applicable law provides.

8.37.070. Construction. This chapter does not limit visual comparison of images by a person, the performance of duties imposed by State law, or compliance with a judicial warrant, court order, or subpoena.

8.37.080 Implementation. The chief of police may adopt administrative rules, policies, procedures, and general orders to implement this chapter, including those that are more restrictive than this chapter requires."

SECTION 3. This Ordinance takes effect on approval.

paf:zcs:26-239a

INTRODUCED BY:

Tamara A.M. Paltin

TAMARA PALTIN