# USING FACIAL RECOGNITION SYSTEMS

Policy #808-R03 (12/13/18)

*Applies to all staff granted access to WCSO facial recognition technology.*

*The Sheriff's Office recognizes that facial recognition technology is a powerful tool to assist with identification and enhance public safety, and that it can present significant privacy implications if used inappropriately. The intent of this policy is to provide rules for when and how facial recognition may be used and to safeguard the public from unnecessary surveillance and unwarranted privacy intrusions.*

**Definitions.**

**Facial recognition technology**. A computer application capable of comparing specific physical features of a person depicted in a digital probe image against a database of images of persons identified through other means.

**Facial recognition search result**. An image returned by facial recognition technology that represents a potential investigative lead based on an algorithmic similarity to the submitted image.

**Mass surveillance**. The use of facial recognition tools to record and search facial images of a group of persons in a public place when there is no reasonable suspicion to believe that they have engaged in criminal activity.

**Probe image.** A digital image submitted for analysis and comparison to other images in a facial recognition database.

## FACIAL RECOGNITION PRIVACY AND PROTECTIONS

**1. <u>Staff Will Only Use Facial Recognition Technology Systems Within the Limits of Constitutional and Legal Authority and WCSO Policies</u>.**

- ORS 133.535, *Permissible objects of search and seizure*
- ORS 133.545 through 133.703, *Search warrants*
- ORS 133.033*, Peace officer community caretaking functions*
- With consent of the person
- The Oregon Search and Seizure Manual
- Staff will not employ this technology without a lawful justification that is based upon a criminal nexus.
- Staff will not employ this technology to conduct mass surveillance.
- Staff will not use this technology to screen individuals, places, groups, or activities, unless doing so in accordance with this policy and applicable case law.
- Policies prohibiting biased policing also apply to the use of facial recognition. Facial recognition cannot be used to conduct surveillance of persons or groups based solely on their religious, political or other constitutionally protected activities, their race, ethnicity, gender, or sexual orientation.

**2. Absent Other Evidence, a Facial Recognition Search Result Alone Will Not Constitute Probable Cause for Arrest or to Seize Any Person.**
Facial recognition search results are potential leads that require follow-up investigation, such as the verification of a person's true identity and evaluation of the lead in light of other information and facts.

## ACCEPTABLE USES OF FACIAL RECOGNITION SYSTEMS

**3. Facial Recognition Searches May be Used to Identify Criminal Suspects Caught on Camera.**
Deputies may use facial recognition as an investigative tool when a deputy has reasonable suspicion that the person has committed a crime or when a deputy believes the person is a victim of a crime.

**4. Deputies May Run Facial Recognition Searches in the Field Via a Mobile Device to Help Confirm Identification.**
Deputies may use facial recognition in the field to help confirm a person's identity—

- When an individual consents to have his or her photograph taken for the purpose of identification. If consent is withdrawn, use of facial recognition is not authorized and its use must stop immediately (unless another justification applies).
- When a deputy is unable to confirm an individual's identity and has reasonable suspicion that the individual has committed a crime; if verifying the person's identity could provide a resolution other than a custodial arrest.
- When a person is unable to provide reliable identification due to physical incapacitation or defect, mental incapacitation or defect, or death, and immediate identification is needed to assist the deputy in the performance of lawful duties.

**5. When an Individual is Under Arrest and Their Identity is Unknown, Facial Recognition May be Used to Help Staff Ascertain Correct Identification by Determining Whether the Suspect has been Previously Booked at the Washington County Jail for a Crime.**
The Automated Fingerprint Identification System may also be used in such cases to help staff determine correct identification.

**6. Facial Recognition May be Used in Response to a Significant Threat to Life.**
Deputies may use facial recognition technology immediately while investigating a crime against persons and —

- When probable cause exists to believe an identified suspect, for whom deputies have a felony arrest warrant, or probable cause to arrest for a felony crime, will be at a specific location on a specific date. Such use will require preapproval by a Sheriff's Office command officer. Deputies will document the cause for use, a description of the application of facial recognition tools, and the outcome in a police report.

  Or

- When deputies have reasonable suspicion that a suspect is engaged in or about to be engaged in an act of terrorism as defined by the Homeland Security Act of 2002, and that suspect will be at a specific location within a defined period of time or dates. Such use will require preapproval by a Sheriff's Office command officer. Deputies will document the cause for use, a description of the application of facial recognition tools, and the outcome in a police report.

## DATABASE AND DATA LIMITATIONS

**7. WCSO Facial Recognition Technology Runs Searches Against a Database of Washington County Jail Booking Photos (Mugshots) Dated From 2001 to Present.**
Automated Custody Management System technology removes expunged jail booking photos daily from the facial recognition database; this process will be reviewed as part of the annual audit.

## TRAINING

**8. Only Authorized WCSO Staff Who Have Been Trained May Access or Use Facial Recognition Technology.**
Initial training will cover proper and lawful use of the technology as outlined in WCSO policy. Periodic training will be provided as appropriate for technology advances or policy updates.

## DOCUMENTATION AND PENALTIES FOR MISUSE

**9. As With Other Restricted Investigative Resources, Deputies Must Document Appropriate Justification for the Use or Request of a Facial Recognition Search**.

- Appropriate justification will include the purpose for the search, a case number or incident number when available, or a brief description of the situation when available.
- For searches conducted on behalf of another investigator, deputies will document the name, law enforcement agency, and job title of the requestor in a report or in their duty notebook.
- Penalties for misuse may include, but are not limited to, termination of a user's access to facial recognition technologies or the termination of agency-wide access to the system, or discipline as appropriate.

## RECORDS RETENTION AND EXPUNGEMENTS

**10. Probe Images Will be Maintained in Accordance With Relevant WCSO Policy and the WCSO Evidence Manual, and Will be Saved on a Washington County Controlled and Maintained Server.**

- Probe images are saved using a generated unique identifier and have no personal identifying information.
- Probe images that result in or are connected to a criminal case will be maintained as criminal evidence in accordance with the Oregon State Archivist's record retention rules.
- Probe images that do not result in or become connected to a criminal case will be saved for one year after the search, and then purged from the server.
- Automated Custody Management System (CMS) technology removes expunged jail booking photos daily from the facial recognition database; this process will be reviewed as part of the annual audit.

## ANNUAL AND PERIODIC AUDITS

**11. All Facial Recognition Use and Search Requests are Subject to Audit.**

- A Patrol Commander will appoint a lieutenant to perform an annual audit of WCSO use of facial recognition.
- At a minimum, the audit will include a review of policy compliance by users, a review of complaints involving facial recognition, and offer recommendations for training, policy, or program improvement. The audit will also confirm the automated CMS process for removing expunged jail booking photos from the facial recognition database.

- A written audit report will be submitted to the Sheriff via the chain of command by January 31 each year. The WCSO Law Enforcement Technology Unit may assist the audit process.

## REFERENCES

WCSO Directives:
Policy 207, *General Conduct – Protection of Records*
Policy 1415, *Criminal Investigations – Complying with 28 CFR Part 23*
Criminal Investigations and Case Assignment Manual – *Eyewitness Identifications*

## RESOURCES

Bureau of Justice Administration, 28 CFR Part 23, *Guide to Criminal Intelligence Policies*