Frontier Institute
PO Box 5104
Helena, MT 59604
406.924.9763
frontierinstitute.org

Frontier Institute Comment: HJ 48

Chairman Bogner and Committee Members,

Facial Recognition Tech (FRT) is increasingly being used as a tool to make Montana government more efficient - assisting law enforcement investigations and rooting out identity fraud. However, this powerful technology can be abused, threatening the privacy and security of Montanans without proper public knowledge and oversight.

Frontier Institute identifies two main concerns with the current system regulating the use of FRT by governments in Montana:

1. No uniform standard for the use of FRT by law enforcement

After a series of public information requests, Frontier Institute understands that the Montana Analysis and Technical Information Center (MATIC)[1] – the state's fusion center[2] – has an internal policy governing the use of FRT. While MATIC does not have direct access to a FRT system, it is authorized to submit search requests to external entities with FRT system access. Under the policy, FRT searches are authorized only for specific use cases, with investigations conditioned on "reasonable suspicion" of a crime.

However, the MATIC policy applies only to FRT searches they facilitate. Recent media reports revealed that local Montana law enforcement agencies directly ran potentially hundreds of FRT searches using a separate system.[3]

The existence of internal policies governing local law enforcement use of FRT is unknown to the public, leaving open questions about the adequacy of internal policy to protect against abuse.

Recommendation #1

The Legislature should consider adopting a transparent, uniform standard for FRT use by law enforcement in Montana. The uniform standard should establish the necessary legal conditions for investigations or searches which utilize FRT (reasonable suspicion, probable cause etc.)

---

[1] https://dojmt.gov/enforcement/investigations-bureau/
[2] https://www.dhs.gov/national-network-fusion-centers-fact-sheet
[3] https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table

2. No uniform standard for accessing civilian FRT databases

FRT is already used for identity verification in non-criminal contexts, such as Unemployment Insurance (UI) and the Department of Motor Vehicles (DMV).

The DMV has maintained that they do not allow any external access to their FRT system. However, the Montana's driver's license database is shared with national law enforcement databases, such as the National Law Enforcement Telecommunication System (NLETS)[4]. NLETS intends[5] to develop FRT search capabilities, which may in the future subject law-abiding driver's license holders to law enforcement FRT searches.

The use of third-party FRT applications also opens significant concerns for law enforcement "backdoors" into civilian FRT databases. For example, Montana's UI Program utilizes the vendor ID.ME for FRT identity verification. ID.ME product terms state that user information can be shared in response to government requests[6]. This vendor policy could mean that, despite the existence of any internal UI FRT system use policy, law enforcement may be able to access FRT searches of the UI database via requests to the vendor.

These examples pose concerns about the security and privacy of law-abiding citizens who apply for government benefits or receive a driver's license in Montana.

Recommendation #2

The legislature should consider adopting a transparent, uniform standard for FRT system access in non-criminal contexts. The uniform standard should establish authorized law enforcement uses of civilian FRT databases and extend those same conditions to any FRT vendors. Photos collected in FRT databases in a non-criminal context should not be automatically linked or shared with any external law enforcement database.

Frontier Institute encourages the committee to scrutinize government use of FRT in Montana and evaluate the necessity of adopting a transparent, uniform standard for its use.

Thank you,

Kendall Cotton

Kendall Cotton
President and CEO

---

[4] https://www.nlets.org/resources/maps/initiatives/key
[5] https://www.nlets.org/sites/default/files/2021-05/baa_fact-sheet.pdf
[6] https://www.id.me/privacy

Montana Analysis and Technical Information Center
Policies and Procedures

Section: INTELLIGENCE
Policy Number: K-13
Policy Name: MATIC FACIAL RECOGNITION POLICY
Effective Date: 12/16/2020
Revised Date:

I. Purpose

A. The mission of the Montana Analysis and Technical Information Center (MATIC) is to collect, store, analyze and disseminate information on public safety issues, including suspected offenses, to the law enforcement community and government officials regarding dangerous drugs, fraud, organized crime, terrorism and other criminal activity for the purposes of decision making, and proactive law enforcement while ensuring the rights and privacy of citizens.

B. It is the purpose of this policy to provide MATIC personnel with guidelines and principles for the requests for facial recognition. This policy will ensure that all uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties (P/CRCL) of individuals.

C. Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face using biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. MATIC has established this policy to support the investigative efforts of Montana law enforcement and public safety agencies.

D. The MATIC does not have direct access to a facial recognition system. Personnel may request a facial recognition search via systems maintained by other law enforcement entities for valid law enforcement purposes and criminal case support.

E. This policy assists MATIC and its personnel in:
- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.

- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of criminal investigations, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

F. All deployments of the face recognition requests for information are Unclassified//Law Enforcement Sensitive/For Official Use Only (U//LES/FOUO). The provisions of this policy are provided to support the following authorized uses of face recognition information:
   - A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal conduct or activity.
   - An active or ongoing criminal investigation.
   - To mitigate an imminent threat to health or safety.
   - To assist in the identification of a person who lacks capacity or is otherwise unable to identify him or herself.

G. All personnel, participating agency personnel, and authorized individuals working in direct support of the fusion center and other authorized users will comply with this facial recognition policy. An outside agency, or investigators from an outside agency, may request facial recognition searches to assist with investigations only if the outside agency is making the request based on a valid law enforcement purpose that falls within the authorized reasons in this policy.

H. The law enforcement requestor must provide a case number, crime type, contact information (requestor's name, requestor's agency, and phone number), and acknowledges an agreement with the following statement:

> *The result of a face recognition search is provided by MATIC only as an investigative lead and is NOT to be considered a positive identification of any subject. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.*

I. All MATIC personnel, participating agency personnel, and authorized individuals working in direct support of the MATIC and other authorized requestors will comply with applicable laws including the MATIC Privacy Policy as well as all applicable state and federal P/CRCL laws.

II. Governance and Oversight

The Montana Department of Justice, Division of Criminal Investigation has the primary responsibility for the operation of the MATIC, including:

- Coordination of personnel;
- The collection, receipt, retention and evaluation of information;
- The analysis, destruction, sharing or disclosure of such information.

The MATIC's Supervisor will work with the MATIC Privacy Officer to oversee the following responsibilities for facial recognition requests:

- Oversee and administer the face recognition requests to ensure compliance with applicable laws, regulations, standards, and policy.
- Ensuring that personnel (including investigators from external agencies who may make face recognition requests) meet all prerequisites stated in this policy prior to processing a request and have a valid need-to-know and right-to-know.

The Criminal Intelligence Information Advisory Council (CIIAC) can request an audit of the MATIC and its personnel to verify compliance of this facial recognition policy. The CIIAC is outlined in Montana Code Annotated 44-5-501 through 44-5-515.

III. Acquiring and Receiving Face Recognition Requests

A. MATIC is authorized to submit facial recognition search requests to be performed by external law enforcement entities that own and maintain face image repositories. For the purpose of performing face recognition searches, MATIC will obtain probe images from authorized requesting agencies only for the authorized uses identified in this policy.

B. MATIC and, if applicable, any authorized requesting or participating agencies will not violate First, Fourth, and Fourteenth Amendments and will not perform or request face recognition searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

IV. Use of Face Recognition Information

A. Access to or disclosure of face recognition search results will be provided only to individuals within the entity or in other governmental agencies who are authorized to have access and only for valid law enforcement purposes with a right-to-know and need-to-know.

B. MATIC will prohibit assistance to law enforcement agencies for requests for facial recognition assistance, including dissemination of face recognition search results, for the following purposes:
   - Non-law enforcement (including but not limited to personal purposes).
   - Any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments.
   - Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
   - Harassing and/or intimidating any individual or group.
   - Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

V. Sharing and Disseminating Face Recognition Information

A. MATIC personnel will log all facial recognition requests in compliance with other MATIC policies and procedures.

B. Each request must be accompanied by a case number, investigator's contact information, and the crime type (ex. homicide, theft, sexual assault, etc.) prior to processing the request to verify right-to-know and need-to-know.

VI. Data Quality Assurance

A. Original probe images will not be altered, changed, or modified in order to protect the integrity of the image.

B. MATIC considers the results, if any, of a face recognition search to be advisory in nature as an investigative lead only. Face recognition search results are not considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods by the investigating agency.

C. All potential matches are considered advisory in nature and any subsequent verification of the individual's identity, such as through a fingerprint check, or follow-on action should be based on the requesting agency's standard operating procedures.

VII. Complaints

A. If an individual has a complaint with regard to face recognition information that is exempt from disclosure, the MATIC Supervisor or Privacy Officer will notify the originating agency within 30 days in writing or electronically and, upon request,

assist such agency to correct any identified data/record deficiencies in the information or verify that the record is accurate.

B. The MATIC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens the physical well-being, reputation, or finances of the person. The notice will be made promptly and without unreasonable delay following discovery of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release, and will follow the guidance set in the MATIC's Privacy Policy.

VIII. Information Retention and Purging

A. MATIC is authorized to submit face recognition search requests to external agencies that own and maintain face image repositories. The images searched are subject to the retention policies of the respective agencies that maintain or own the face image repositories.

B. Once a face recognition image is downloaded by law enforcement personnel and incorporated into a criminal intelligence record or an investigative case file, the face recognition information is then considered criminal intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or criminal intelligence govern its use.

C. Any images that do not originate with MATIC will remain in the custody and control of the originating agency and will not otherwise be transferred to any other entity without authorization from the originating agency.

IX. Accountability and Enforcement

A. MATIC will be open with the public on this policy and will provide a copy upon request.

B. The MATIC Supervisor or designee will be responsible for receiving and responding to inquiries and complaints about the entity's use of the face recognition system, as well as complaints regarding incorrect information or P/CRCL protections. Public inquiries can be mailed to the **MATIC Supervisor at PO Box 201417 Helena, MT 59620-1417**.

C. MATIC will adopt and follow procedures and practices by which the fusion center can ensure and evaluate the compliance of personnel with the provisions of this policy and applicable law.

D. If MATIC personnel, a participating agency, or an authorized requestor is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the MATIC Administrator or designee will:
    - Suspend or discontinue access to information by MATIC personnel, the participating agency, or the authorized requestor.
    - Apply appropriate disciplinary or administrative actions or sanctions.
    - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

E. MATIC reserves the right to establish the qualifications and number of personnel having access to request face recognition requests for information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this face recognition policy.

Glossary of Terms and Definitions

Authorization—The process of granting a person, a computer process, or device with access to certain information, services, or functionality.

Biometrics—A general term used alternatively to describe (1) a characteristic or (2) a process—(1) a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition or (2) automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.14

Center—See Fusion Center.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of

Civil Rights—The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federal- or state- protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.16

Collect—For purposes of this document, "gather" and "collect" mean the same thing.

Comparison—The observation of two or more faces to determine the existence of discrepancies, dissimilarities, or similarities.

Confidentiality—Refers to the obligations of individuals and institutions to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies. See Privacy.

Criminal Activity—A behavior, an action, or an omission that is punishable by criminal law.

Criminal Case Support—Administrative or analytic activities that provide relevant information to law enforcement personnel regarding the investigation of specific criminal activities or trends or specific subject(s) of criminal investigations.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Dissemination—See Disclosure.

Face Recognition—The automated searching for a reference image in an image repository (see Repository) by comparing the facial features of a probe image with the features of images contained in an image repository (one-to-many search). A face recognition search will typically result in one or more most likely candidates—or candidate images—ranked by computer-evaluated similarity or will return a negative result.

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, including investigative information; tips and leads data, including suspicious activity reports; and criminal intelligence information.

Investigative Lead—Any information which could potentially aid in the successful resolution of an investigation but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

Law Enforcement Information—law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

Personally Identifiable Information (PII)— Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual.

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of PII.

Privacy Policy—Short term for a privacy, civil rights, and civil liberties (P/CRCL) policy which is a printed, published statement that articulates the policy position of an organization on how it handles the PII that it gathers or receives and uses in the normal course of business.

Request—A request received by MATIC to utilize face recognition in support of a criminal investigation. Submissions will not contain original evidence.

Right to Know—A requirement for access to specific information to perform or assist in a lawful and authorized government function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity, or the roles and responsibilities of particular personnel in the course of their official duties.