Policing Project
NYU School of Law

NYU School of Law
40 Washington Square South
New York, NY 10012

info@policingproject.org
@policingproject
212.992.6950

To: Members of the Economic Affairs Interim Committee

From: Katie Kinsey, Staff Attorney, The Policing Project at NYU School of Law

Date: July 13, 2022

Re: HJ 48 – Written Comments on the Need to Regulate Ongoing Law Enforcement Use of Face Recognition Technology

---

Members of the Economic Affairs Interim Committee:

Thank you for the opportunity to submit testimony at this hearing to address government use of face recognition technology (FRT) in Montana. My name is Katie Kinsey, I am a staff attorney at the Policing Project at New York University School of Law, an organization dedicated to partnering with communities, policymakers, police, and technology companies across the country to bring democratic accountability to policing. By democratic accountability we mean that the public has a voice in setting transparent, ethical, and effective policing policies **before** the police act. This hearing is a great example of democratic accountability in action, and I am grateful to participate.

Having reviewed this committee's draft bill to regulate government use of FRT, it is clear that you already have thought deeply about the thorny issues raised by this technology. We have as well. Over the past year, we convened a diverse group of stakeholders (including law enforcement, civil liberties advocates, and technology vendors) for hours of discussion on law enforcement use of FRT. These discussions cemented our belief that if law enforcement is going to continue to use FRT, there must be comprehensive legislation in place to help ensure use of this technology improves public safety and does not involve violations of fundamental rights.

To help guide legislative bodies considering regulating police use of FRT, we have developed a checklist of minimum regulatory guidelines. We were heartened to see many of these essential guidelines echoed in your draft bill. We have provided a copy of this checklist to the committee as a resource for your consideration.

In my testimony today, I want to make three overarching points:

1. Unregulated law enforcement use of FRT is a recipe for harm. If law enforcement agencies in Montana are going to continue to use FRT, Montana should join more than a dozen states in passing legislation that establishes guardrails on agencies' use.

2. The public deserves to know whether law enforcement's use of FRT actually makes the public safer. If this body authorizes law enforcement use of FRT, it should be authorized only for a limited pilot phase during which time its impact on public safety—both its advantages as well as its harms and risks—can be evaluated.

3. It is our view that to facilitate the responsible use of FRT, its use should occur though a single agency. In that way, officials can be trained properly and necessary protocols developed and observed. This also would facilitate an assessment of whether FRT improves public safety and at what cost.

I. If law enforcement is going to use FRT, its use must be strictly regulated

As this committee's work has revealed, law enforcement agencies in Montana are using FRT despite there being no laws in place to regulate this use. Police use of FRT without any guardrails raises serious concerns, namely:

- **Accuracy and bias issues:** Because of inadequate or nonexistent testing, the accuracy of FRT as used by law enforcement is entirely unproven. Research continues to show that FRT can be less accurate when attempting to identify women, the elderly, and especially people with darker skin. Already, unregulated law enforcement use of FRT has contributed to misidentifications that resulted in false arrests. Although testing under laboratory conditions shows some improvement in the quality of FRT algorithms, we are entirely in the dark about how this technology operates under real conditions. The two are not comparable and one cannot assume the performance in the laboratory tells us much about performance under actual law enforcement conditions. There are very real risks here.

- **Risks to free expression:** Police have used FRT to target individuals exercising their First Amendment rights, raising serious concerns about creating chilling effects on constitutionally protected activity.

- **Privacy risks:** FRT supercharges current police surveillance capabilities by facilitating searches of databases of millions of faces (including social media images scraped from the internet without individuals' consent) in a matter of seconds. Combined with ever-increasing networks of public and private surveillance cameras, FRT can enable governmental surveillance and tracking with unthinkable speed at an unprecedented scale, with no ability to opt out. After all, you can't leave your face at home. History makes clear that without meaningful legislation reining in police use of FRT—including explicitly banning FRT for real-time or historical tracking—there will be misuse.

Concerns like these have led lawmakers in states like Colorado and Utah to pass legislation limiting law enforcement's use of this powerful technology. In short, Montanans will be safer if you pass legislation like the draft bill in front of this committee.

II. Legislation should limit use to a pilot phase during which public safety impact is assessed

At the Policing Project, our evaluation of any policing technology starts with a basic question: will the public benefit from the use of this tool? If a technology has identifiable, concrete benefits then we can begin to address costs and ways to mitigate them before it is used.

Current law enforcement use of FRT has inverted this analytical process – applying a deploy first, assess benefit later (if ever) approach. The public deserves to know whether this technology actually works, and agencies that use (or want to use) this tool should bear the burden to proof to show that it does. What is needed is a full accounting of how FRT is being used, and an evaluation of the technology's impact on public safety. This evaluation should include a real commitment to stop use if the public safety benefits do not outweigh the costs, or the most serious costs – such as those to racial justice interests – cannot be mitigated.

As our checklist makes clear, legislation can facilitate meaningful assessment of FRT's public safety impact by requiring comprehensive data collection on agency use during a pilot period. The careful, transparent data collection envisioned will enable an assessment of benefits and costs and, in turn, public safety impact.

III. Centralize FRT use in a single state agency

We strongly recommend that this body consider centralizing FRT use in a single state agency that is subject to public oversight rather than permit individual agencies to conduct their own searches. Centralization offers a number of benefits and protections. It would facilitate the comprehensive data collection and assessment needed during the pilot phrase and enable easier auditing and oversight of agency use rather than placing these administrative burdens on individual agencies. It also would enable consistent training standards and use protocols and consolidate expertise. Other states are embracing this approach. For example, a Massachusetts legislative commission tasked with evaluating law enforcement use of face recognition in that state recently recommended centralization, finding that it "will promote efficiency, ensure consistency, improve training and foster more accountability and transparency."[1] In short, ensuring that FRT use occurs under one (publicly accountable) roof, where the same rules and procedures apply, will make it easier to monitor for and protect against abuse and misuse.

Thank you again for the opportunity to testify today. The matter you are considering is extremely consequential. We would be happy to provide any other information that could be useful.

[1] Final Report, Special Commission to Evaluate Government Use of Facial Recognition Technology in the Commonwealth, at 31-32 (March 14, 2022), https://frcommissionma.files.wordpress.com/2022/03/fr-com-final-report-appendices-3.14.22.pdf.

Policing Project
NYU School of Law

Working Draft

WHY ONGOING LAW ENFORCEMENT USE OF FACE RECOGNITION TECHNOLOGY MUST BE REGULATED - NOW

THE PROBLEM

Law enforcement agencies across the country are adopting and using face recognition technology (FRT) without explicit statutory or democratic authorization, posing real risks to our civil rights and civil liberties. If policing agencies are going to continue to use this technology, this use must be subject to carefully-considered regulatory guardrails.

Persistent Accuracy and Bias Concerns

FRT presents significant accuracy and bias concerns. Because of inadequate or nonexistent testing, the accuracy of FRT as used by law enforcement is entirely unproven. Research has shown that many algorithms may exhibit higher error rates when attempting to identify women, minors, and especially people with darker skin. Although testing under laboratory conditions shows some improvement in the quality of FRT algorithms, we are entirely in the dark about how this technology operates under real-world conditions. The two are not comparable and one cannot assume the performance in the lab tells us much about performance under actual law enforcement conditions.

Racial bias concerns are not limited to the algorithms, rather, racial disparities in the criminal legal system infect the entire FRT process. Communities of color have been and continue to be subject to disproportionate criminal enforcement—from stops, to searches, to arrests. This means that people of color are overrepresented in many of the databases police use to conduct FRT searches. Taken together, continued disproportionate enforcement against people of color combined with searching databases containing disproportionately more faces of color means these communities will bear the brunt of FRT's harms. Already, unregulated law enforcement use of FRT has contributed to misidentifications that led to false arrests. To date, every single person wrongly arrested because of FRT has been a Black man.

Risks to Free Expression and Privacy

Police also have used FRT to target individuals exercising their First Amendment rights, including at racial justice protests and during Juneteenth celebrations, raising serious concerns about creating a chilling effect on constitutionally protected activity. This type of FRT use also evokes historical government surveillance practices targeting political dissidents and marginalized

communities, from the FBI's spying on civil rights leaders in the 1960s to the NYPD's secret videoing of mosques after 9/11.

FRT supercharges current police surveillance capabilities by facilitating searches of databases of millions of faces (including social media images scraped from the internet without individuals' consent) in a matter of seconds. Combined with ever-increasing networks of public and private surveillance cameras, FRT can enable governmental surveillance and tracking with unthinkable speed at an unprecedented scale, with no ability to opt out. After all, you can't leave your face at home. History makes clear that without meaningful legislation reining in police use of FRT, there will be misuse, particularly against people of color.

THE SOLUTION

We need a new approach: one that is informed by the democratic process and that ensures police only may use the technology if it makes the public safer, if the public actually wants it, and if the technology does not perpetuate harms like racial injustice and invasions of privacy. Legislative bodies should enact comprehensive regulation to strike this balance. Our legislative checklist presents a way forward, namely a set of minimum guidelines for comprehensive regulation of this powerful technology.

WHAT THE CHECKLIST DOES

Establishes democratic authorization as the baseline

The checklist insists that a regulatory framework, approved by a democratically-accountable body, must be in place for police to use FRT.

Requires absolute transparency about police use of FRT

The checklist establishes reporting and auditing requirements around police use of FRT to enable public oversight and evaluation of its benefits and harms.

Limits the uses of FRT

The checklist sets strict limits on permitted uses of FRT, restricting searches to certain serious offenses and clarifying which uses are never allowed, like using FRT for surveillance.

For permitted uses, the checklist outlines specific guardrails for deploying FRT, such as requiring a warrant to conduct searches. These limitations ensure that legislation can both allow FRT as a valuable investigatory tool and safeguard the public's constitutional rights.

Mandates testing protocols and accuracy benchmarks

The checklist ensures that law enforcement are permitted to use only the most accurate technology available verified through independent, expert testing. Additionally, it includes a requirement that these systems be tested in real-world conditions—"operational testing"—to make sure the public knows whether and how well this technology actually works.

Requires training for officers using and analyzing FRT

A key component of the checklist is to require that police officers who analyze and use FRT results receive adequate training. Training officers on the sources of error and bias that can impact the process will help ensure accuracy.

Policing Project
NYU School of Law

Working Draft

MINIMUM REQUIREMENTS FOR LAW ENFORCEMENT USE OF FACE RECOGNITION TECHNOLOGY FOR FACE IDENTIFICATION: A LEGISLATIVE CHECKLIST

Many states and localities actively are considering regulating police use of face recognition technology (FRT). If policing agencies are going to continue to use this technology, this use must be subject to carefully-considered regulatory guardrails. This document provides lawmakers with an outline of minimum legislative requirements to guide the development of a comprehensive regulatory framework for the most common law enforcement use of FRT: attempting to identify a witness, victim, or person suspected of committing a crime from an image, or "face identification." The checklist is written for lawmakers at any level of government. Items specific to state legislation are in **bold**; items specific to federal legislation are underlined. Although lawmakers may decide to exceed this checklist, everything in it is essential.

I. Democratic Authorization Framework

(1) Use of FRT by law enforcement should be banned unless authorized by a democratically-accountable body.

(2) **Legislation should centralize all FRT use in a single state agency.**

   a. **If individual agencies are permitted to use FRT, such use must be approved specifically by the local democratically-accountable body**.

(3) Legislation should authorize FRT only for a limited pilot period, during which time its impact on public safety—both its advantages as well as its harms and risks—should be evaluated, with opportunities for community feedback, before continued use is authorized. Absent explicit re-authorization by the original authorizing body, FRT use should not be permitted beyond the pilot period.

II. Transparency and Databases

(4) Require specific legislative authorization for the databases that agencies may search or access for FRT ("enrollment databases").

   a. If non-law enforcement databases are authorized—for example, department of motor vehicle image databases—the public should be provided explicit notice (such as conspicuous notices posted at public-facing agency offices and on agency web sites) that law enforcement may use these databases for face recognition searches in criminal investigations.

(5) Require that, at least annually, law enforcement databases used for FRT searches are purged of any images of individuals who have been released after criminal charges were dropped or dismissed or who were acquitted of a charged offense.

(6) Prohibit policing agencies from conducting FRT searches on any enrollment database composed of privately owned images, including but not limited to any enrollment database that contains images from social media platforms.

(7) Require that any policing agency that uses FRT have and make public a comprehensive use policy, developed with an opportunity for public review and comment.

(8) Require that agencies track complete details of FRT use in each individual case and include this information in the case file.

(9) Require that agencies publish, at least annually, a report summarizing their FRT use, including aggregated data tracked for individual cases (see #8).

(10) Require that agencies conduct and make public annual audits of their use of FRT, including demographic breakdowns of the searches conducted, to ensure use complies with all applicable laws and policies.

III. Testing

International standards and best practices recommend three types of testing for FRT systems—each serving a distinct purpose: (1) **technology testing** to assesses the performance of the FRT algorithm; (2) **scenario testing** to simulate an actual use case; and (3) **operational testing** to assesses an FRT system in a real-world deployment context. To facilitate this:

Congress should direct and empower the National Institute of Standards and Technology (NIST) to:

(11) Develop a benchmark test that implements the following four requirements:
   a. Evaluates the FRT algorithms actually sold to law enforcement;
   b. Evaluates the types of images commonly used by law enforcement, such as surveillance cameras images;
   c. Searches demographically representative, larger enrollment databases; and
   d. Reports error rates by demographic groups.

(12) Develop a scenario testing program that simulates common law enforcement investigative use applications in order to provide insight into potential sources of error for these applications and inform guidelines for real-world use.

(13) Develop an operational testing protocol that agencies can use to assess how effective, equitable, and accurate their FRT systems are when actually deployed.

WHAT IS NIST?

The National Institute of Standards and Technology (NIST), housed in the U.S. Department of Commerce, is the nation's leading physical sciences laboratory. Its mission is "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology."

For the past two decades, NIST has led federal government efforts to develop standards for emergent biometrics and AI technologies. As part of this work, NIST has created field-leading benchmark evaluations of face recognition algorithms. Its expertise and experience with technical assessment of face recognition systems is unrivaled.

(14) Require that agencies only procure FRT from a vendor that the appropriate administrative body determines, using results from NIST's technology testing on low-quality probe images, has demonstrated high accuracy across demographic groups for the intended use case and use population(s).

(15) Require at least annual operational testing of FRT systems as actually deployed to ensure low real-world error rates for the intended use populations. Results should be made publicly available in concise, clear, and accessible language to enable review by a nontechnical audience and with the context necessary to understand the applicability and limitations of these assessments.

a. This testing should be conducted either by independent, expert third-party testers (such as a biometrics testing lab or qualified academic lab) or according to a legislatively-approved protocol developed by independent experts (such as a NIST-developed protocol).

IV. Officer Training

(16) Require that all individuals who review, analyze, use and interact with the FRT system(s) receive specialized training on the capabilities and limitations of this technology generally and the particular system(s) in use.

(17) Require that FRT results be subject to review by a trained officer before a possible match can be determined.

(18) Develop and incentivize the adoption of/**implement** national/**statewide** training standards for individuals who review and analyze the results returned by face recognition

algorithms, (commonly referred to as the "humans-in-the-loop") before those results are shared with law enforcement investigators.

V. Procedural and Categorical Limits

(19) Limit FRT searches to the investigation of serious felony crimes or to identify deceased, incapacitated, or missing persons.

(20) Ban FRT:

a. For use in criminal investigations to identify suspects who are minors;

b. For surveillance—i.e., using real-time or stored video to track people, with or without individualized suspicion, allowing their whereabouts to be traced—unless or until there is proof that legislatures can regulate and control the use of FRT for face identification.

(21) Require a warrant before an FRT search is initiated for criminal investigations, showing that there is probable cause to believe the unidentified person in the submitted photo is involved in one of the uses for which FRT is authorized.

(22) Require a court order before an FRT search is initiated to identify deceased, incapacitated, or missing persons.

(23) Prohibit FRT search results from being considered positive identification or used to establish probable cause for an enforcement action.

(24) Absent exigent circumstances, before arresting an individual identified based on FRT, law enforcement must obtain an arrest warrant or court order that also confirms that all FRT statutory and policy requirements have been followed

VI. Disclosure to the Accused

(25) For any case in which an FRT search was utilized and a criminal proceeding commenced—whether or not a suspect was identified using FRT—require agencies to disclose to the accused, including prior to plea negotiations, complete information around their use of FRT. Such a provision should include meaningful remedies for failure to comply.

VII. Vendor Requirements

Authorizing legislation should require that vendors:

(26) Disclose documentation and information about their FRT systems sufficiently detailed to enable independent, expert assessment of their FRT systems' performance for intended law enforcement use cases.

(27) Ensure their FRT products are self-auditing, i.e., are built with sufficient capabilities such that law enforcement can fulfill all tracking and reporting requirements.

(28) Provide instruction and documentation on image quality and other relevant technical specifications required to maintain low error rates across demographic groups for the particular system(s) sold to law enforcement.

(29) Provide law enforcement agency users with ongoing training, technical support, and software updates needed to ensure their FRT systems can maintain high accuracy across demographic groups in real-world deployment contexts.

VIII. Enforcement

(30) Legislation should include meaningful enforcement mechanisms for statutory violations, such as:

a. **Civil actions** for damages for any person injured as a result of an individual or agency's violation.

b. **Injunctive relief**: the Attorney General/**State Attorneys General** should be empowered to prohibit an agency from using or acquiring any FRT systems, or FRT data where necessary to stop ongoing violations or to prevent future violations.

c. **Administrative remedies**: violations by an employee of a law enforcement agency should be grounds for termination, demotion, or any other appropriate consequences.

d. **Exclusion**: results from unauthorized use and evidence derived therefrom should be excluded as evidence in any trial, hearing, or other judicial or administrative proceeding.

Sullivan, Erin

From: donotreply@mt.gov
Sent: Friday, July 8, 2022 1:22 PM
To: LEG Cmte-EAICcomment
Subject: Public Comment for EAIC

Public Comments for Economic Affairs Interim Committee

Date: 8th July 2022 13:22

First Name:
Dana

Last Name:
May

Email Address:
danamay321@gmail.com

Subject:
Facial Recognition technology

Comment:
I believe we must prohibit facial recognition. This is America, not China. We have the right to privacy. Keep Montana from following the Socialist/ technocratic agenda.

Sent via leg.mt.gov/committees/interim/eaic/public-comments-eaic/

Sullivan, Erin

From: donotreply@mt.gov
Sent: Friday, July 8, 2022 1:32 PM
To: LEG Cmte-EAICcomment
Subject: Public Comment for EAIC

Public Comments for Economic Affairs Interim Committee

Date: 8th July 2022 13:32

First Name:
Betsy

Last Name:
Mancuso

Email Address:
bbwin@bresnan.net

Subject:
Facial Recognition Technology

Comment:
I request that there would be a prohibition of facial recognition technology in the state of Montana. This is yet another disturbing aspect of the ever increasing surveillance state which is a violation of privacy and Amendment 4 of the United States Constitution. As a Montanan, I respect our U.S. Constitution and my privacy, just because this technology exists, does not mean we have to install it, this is not Communist China! - Thank you.

Sent via leg.mt.gov/committees/interim/eaic/public-comments-eaic/

Sullivan, Erin

From: donotreply@mt.gov
Sent: Friday, July 8, 2022 3:18 PM
To: LEG Cmte-EAICcomment
Subject: Public Comment for EAIC

Public Comments for Economic Affairs Interim Committee

Date: 8th July 2022 15:17

First Name:
Virjeana

Last Name:
Brown

Email Address:
jbrown89531@live.com

Subject:
HJ48 study on facial recognition technology.

Comment:
I am opposed to any use of facial recognition technology. There is no privacy anymore. I drive a school bus and am constantly reminding the students to not use their cell phones to take pictures of other students on the bus, especially without the other student's consent. Technology has opened a can of worms and they can't be put back into the can. Everything a person does on-line is already tracked and a person is sent marketing based on internet searches. I personally don't want my pictures all over the internet, and I don't like the idea that some person/business can take a picture and identify myself. I still think we should have a right to our privacy and not have facial recognition used to identify us under any circumstances. Thank you for your time on this issue.

Sent via leg.mt.gov/committees/interim/eaic/public-comments-eaic/

From: donotreply@mt.gov
To: LEG Cmte-EAICcomment
Subject: Public Comment for EAIC
Date: Sunday, July 17, 2022 9:30:26 PM

Public Comments for Economic Affairs Interim Committee

Date: 17th July 2022 21:30

First Name:
Aman

Last Name:
Jabbi

Email Address:
noflaps@gmail.com

Subject:
Facial Recognition (Digital Identity or Digital Dictatorship)

Comment:
Please review video presentation (35 minutes long) to understand the implications of Facial Recognition that will lead to an irreversible dictatorship. Thanks. https://rumble.com/v179jh6-digital-id-or-digital-prison.html

Sent via www.leg.mt.gov/committees/interim/eaic/public-comments-eaic/

From: donotreply@mt.gov
To: LEG Cmte-EAICcomment
Subject: Public Comment for EAIC
Date: Monday, July 18, 2022 3:35:59 PM

Public Comments for Economic Affairs Interim Committee

Date: 18th July 2022 15:35

First Name:
Michelle

Last Name:
Daniels

Email Address:
michelle.daniels40@gmail.com

Subject:
Oppose Facial Recognition Technology in Montana HJ48

Comment:
I strongly oppose Facial Recognition (FR) technology and would strongly encourage you to say “NO” to a surveillance state in Montana. We don’t need to reside in airport style technology in all public and private places in our state nor our country. It 100% infringes on our privacy and individual rights. (FR) “public” cameras must be banned and retracted in Montana. This harmful and controlling technology is used in countries such as China and Russia to track every person without consent or a choice to opt out. Facial Recognition (FR) technology collects and permanently stores data on individuals to establish social scores and a Digital Identity. This surveillance system sees citizens as data. If individuals in these countries disagree with their government, their workplace or the media, they are completely shut down and cut off by technology, and their bank accounts are frozen. We must continually educate ourselves of the high risks of advanced technology in our fast-paced world. IBM’s CEO Arvind Krishna announced last year “IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values." https://edition.cnn.com/2020/06/09/tech/ibm-facial-recognition-blm/index.html . Australian Human Rights Commissioner Edward Santow emphasizes, “This so-called ‘one-to-many’ application of (FR) technology is distinct from the ‘one-to-one’ systems used for passport control or user authentication in smartphones which carried a very low risk of harm. ‘One-to-many’ is much more prone to error and the consequences of error can be exceptionally serious.” https://www.smh.com.au/technology/harm-against-humans-rights-chief-warns-of-facial-recognition-threat-20200611-p551o6.html . In the same article, Dr. Robbie Fordyce, a researcher at Monash University in Melbourne Australia said, “Without proper regulation around where and how data can be collected and stored and for how long, datasets would be

bought and sold between government agencies and private companies — making it impossible for people to understand the use cases even if they consented to their image being stored — and datasets could be conglomerated into central files of personal information." As a Montana resident for 16 years, I strongly oppose FR technology for governmental surveillance in our state. It's too invasive, too expensive, too risky and unlawful to be forced upon Montanans.

Sent via leg.mt.gov/committees/interim/eaic/public-comments-eaic/