Facial Recognition and Artificial Intelligence

Christine T. Chang
PhD Student
Computer Science
University of Colorado Boulder

Tuesday 10 August 2021

Personal Background Highlights

- **Mechanical Engineer** (BS: Cornell University, 7 years experience in government and industry)
- **PreK-20 Educator** (MS: Boise State, 8 years experience at all levels)
- **Computer Scientist** (MS: CU Boulder)
- **PhD Student** in Computer Science (Expected graduation: 2023)
- Former **Volunteer Firefighter** (Nassau Bay VFD / Houston, Texas)

Robert Williams

January 9, 2020:

Arrived home from work to police in his driveway.

Arrested in front of his **wife** and
2 young daughters.

Held overnight at the
Detroit Detention Center.

Interrogated the following morning.

Erroneously identified using facial recognition.

Detained even after the interrogating officer admitted ***“the computer must have gotten it wrong.”***

Finally released approximately 30 hours later.

After ACLU of Michigan filed an **official complaint** and the New York Times wrote an article highlighting this situation, the **Wayne County prosecutor's office** said that Robert Julian-Borchak Williams ***could*** have the case and his fingerprint data expunged.

Impacts

Attendance record at **work**

Financial costs for lawyers

Daughter thought he would **“be right back”**

Long-term **psychological impacts** on his daughters

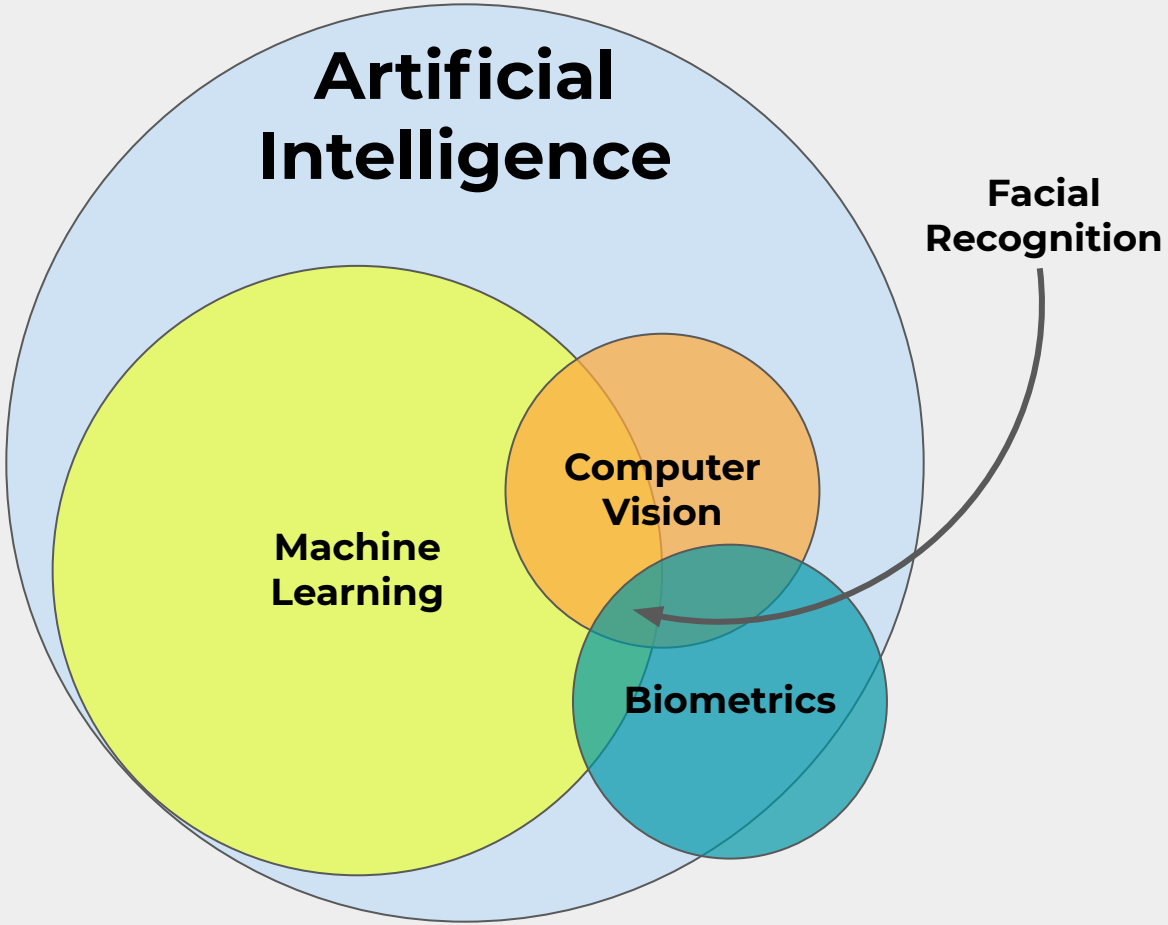
Humans tend to over-trust automated systems, even in high-risk situations and when we have had previous contrasting experiences.

P. Robinette, W. Li, R. Allen, A. M. Howard and A. R. Wagner, "**Overtrust of robots in emergency evacuation scenarios**," 2016 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI), 2016, pp. 101-108, doi: 10.1109/HRI.2016.7451740.

It is clear that we need regulations around the use of facial recognition and other kinds of artificial intelligence (AI).

Outline

A. What are **Artificial Intelligence** and **Facial Recognition**?
B. What are the **potential benefits** of these technologies?
C. What does the research say about their **limitations**?
D. Where does **industry** stand?
E. What is the **current** policy landscape?
F. **Policy Recommendations**
G. Concluding remarks


Artificial Intelligence
Machine Learning
Computer Vision
Biometrics
Facial Recognition

Facial Recognition Overview

1. Detect
2. Analyze
3. Match

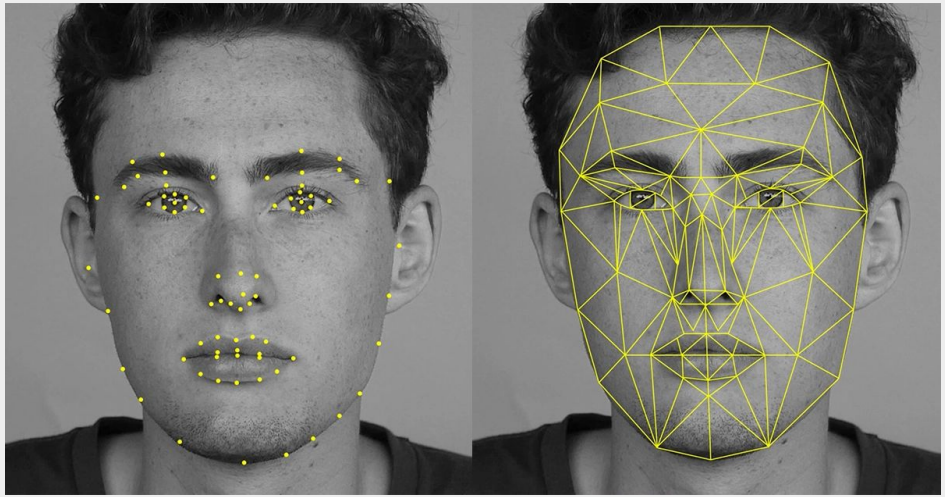
https://www.avigilon.com/products/ai-video-analytics/facial-recognition

1. Detect

https://towardsdatascience.com/face-detection-for-beginners-e58e8f21aad9

➔ Detect faces present in image

2. Analyze



https://petapixel.com/2016/06/30/snapchats-powerful-facial-recognition-technology-works/

➔ Identify facial landmarks
➔ Create faceprint

3. Match

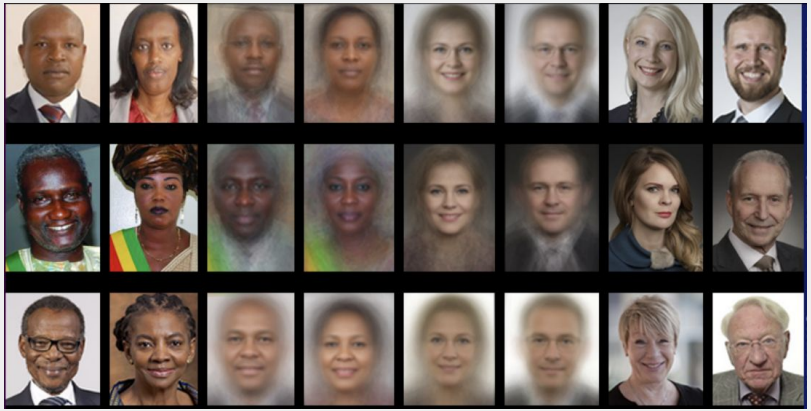
- ➔ Determine if a match exists
  - ➔ Against a single known entity

1:1

https://support.apple.com/en-us/HT208109

  - ➔ Among a database of images

1:N



http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Potential Benefits of Facial Recognition Technology

Easily unlocking your phone

Identification step for building entry

Driver License fraud prevention

Crime investigation

School campus surveillance

Potential Benefits of Facial Recognition Technology

if this technology were 100% accurate and if privacy were 100% assured.

Easily unlocking your phone

Identification step for building entry

Driver License fraud prevention

Crime investigation

School campus surveillance

What does the research say about accuracy & privacy ?

NIST Study

Published December 2019

- **189** mostly commercial algorithms
  - Verification algorithms (1:1)
  - Identification algorithms (1:N)
- **99** developers
- **4** large datasets
- Extremely **detailed** report with extensive descriptions of **methodology** and **results**

What is a “false positive” anyway?

False Positive Identification Rate = $\dfrac{\textbf{\# searches } \textbf{\textit{without}} \text{ an actual mate that } \textbf{return a (false) mate}}{\textbf{\# total searches}}$

“false positive rates are highest in West and East African and East Asian people, and lowest in Eastern European individuals.”

NIST Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects

“With domestic law enforcement images, the highest false positives are in American Indians, with elevated rates in African American and Asian populations.”

NIST Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects

“We found false positives to be higher in women than men, and this is consistent across algorithms and datasets.”

NIST Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects

“We found elevated false positives in the elderly and in children.”

NIST Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects

“...the error rate for one leading algorithm climbed from 0.1% when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured ‘in the wild,’ where the subject may not be looking directly at the camera or may be obscured by objects or shadows.”

Center for Strategic and International Studies
April 2020

June 10, 2020

“We’ve advocated that **governments should put in place stronger regulations** to govern the ethical use of facial recognition technology…

“We hope this one-year moratorium might give Congress enough time to implement appropriate rules, and we stand ready to help if requested.”

June 8, 2020

"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 and Principles of Trust and Transparency.

"We believe **now is the time** to begin a national dialogue on **whether and how** facial recognition technology should be employed by domestic law enforcement agencies."

June 11, 2020

"As a result of the principles that we've put in place, we **do not sell** facial recognition technology to police departments in the United States today...

"...we've decided that we will not sell facial recognition technology to police departments in the United States until we have a national law in place, **grounded in human rights**, that will govern this technology."

But these moratoria by large companies are largely **symbolic**.

It is **smaller or lower profile vendors** who supply a significant portion of facial recognition software to schools, law enforcement agencies, private companies, and other government entities.

“**Schools are the largest market** for video surveillance systems in the U.S., estimated at $450 million in 2018, according to London-based IHS Markit, a data and information services company. The overall market for **real-time video analytics** was estimated at $3.2 billion worldwide in 2018 — and it’s anticipated to grow to **more than $9 billion by 2023**, according to one estimate .”

These vendors are **still marketing and selling** this technology.

Axon

(previously Taser)

AI Ethics Board

- Initiated an independent board
- Members include experts in:
  - AI
  - Computer Science
  - Privacy
  - Law Enforcement
  - Civil Liberties
  - Public Policy
- Two reports:
  - Face Recognition
  - Automated License Plate Recognition

Axon

Ethics Board First Report
June 2019

"**No jurisdiction** should adopt face recognition technology without going through open, transparent, democratic processes, with adequate opportunity for **genuinely representative public analysis, input, and objection**."

Axon

Ethics Board First Report
June 2019

“When assessing the costs and benefits of potential use cases, one **must take into account** both the **realities of policing** in America (and in other jurisdictions) and **existing technological limitations**.”

“Biometrics are usernames, not passwords.”

Tiffany C. Li

Technology Attorney and Legal Scholar
University of New Hampshire
Yale Law School’s Information Society Project

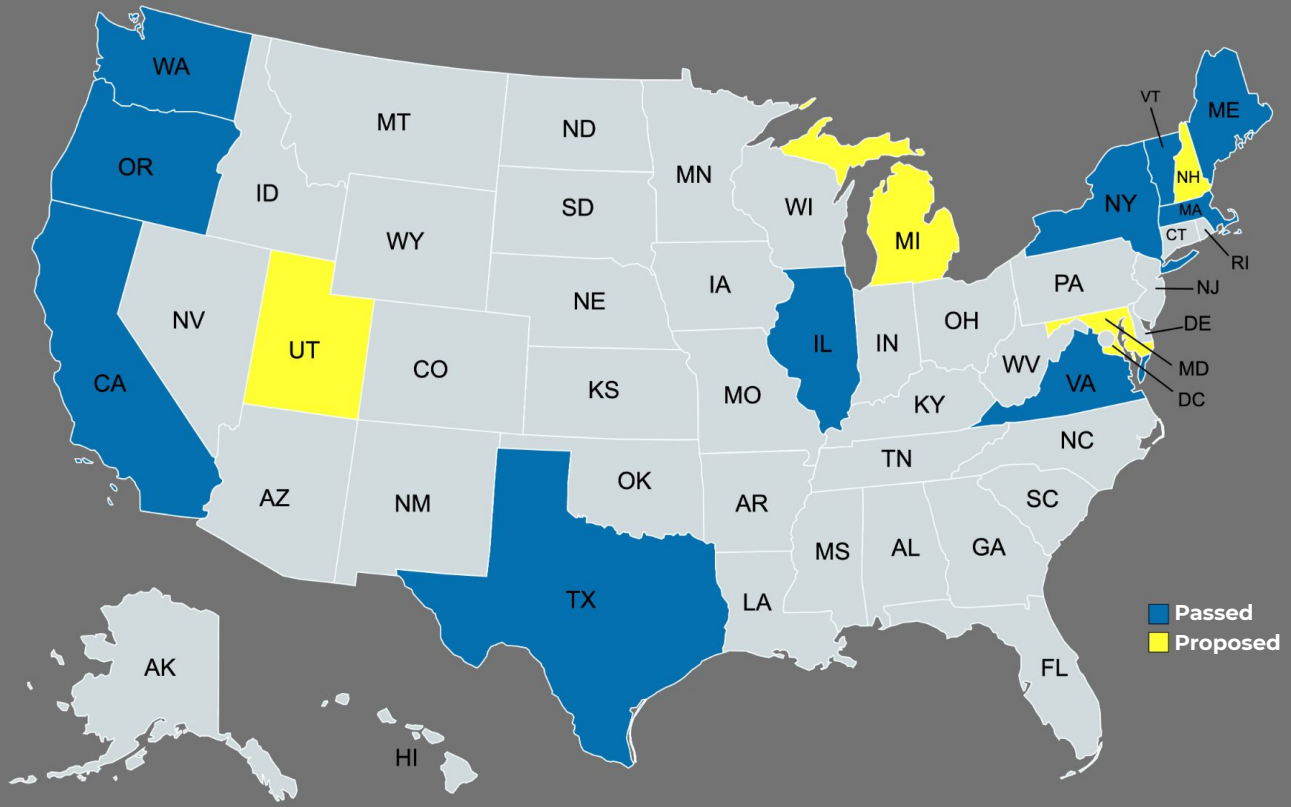
Do we use facial recognition in Colorado?

Yes.

- Colorado State Patrol: to redact video footage from body/dash cameras
- Colorado Bureau of Investigation: to compare suspects from surveillance imagery to state level mugshot databases
- DMV: to detect fraudulent renewals
- Greeley / Weld County School District 6: Avigilon cameras
  - Future upgrades include the ability to identify guns and read people's expressions.

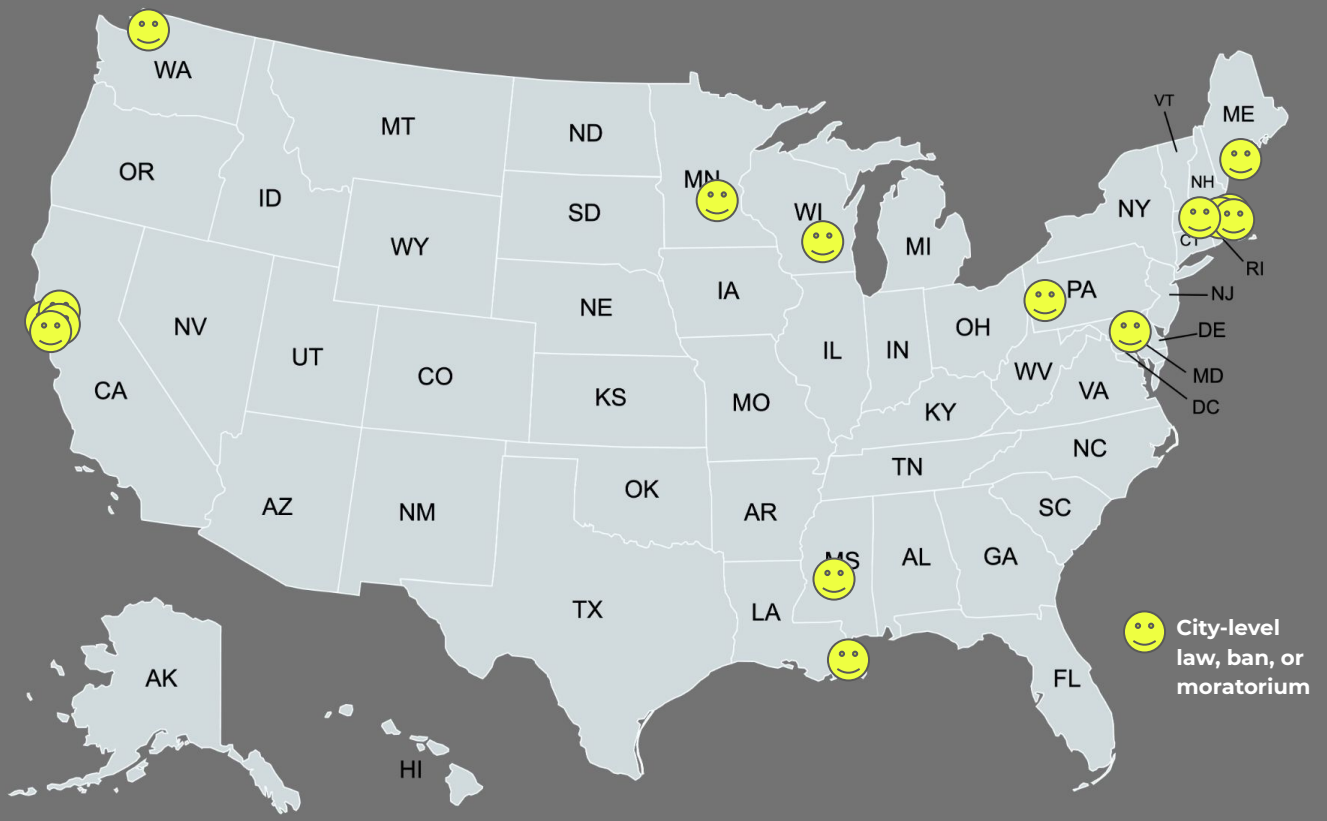
"It will look at the expressions on people's faces and their mannerisms and be able to tell if they look violent."

But we have no laws or statutes around its use.



What are other states doing?

Created with mapchart.net



What about cities?

Created with mapchart.net

Findings After Interviews With Diverse Stakeholders

There is a general need among those at the state government level for a deeper understanding of what artificial intelligence is, what it is capable of, and what its faults are.

Use of facial recognition technology is expanding despite this need for understanding, with privacy and ethical implications.

Policy Proposals

1. **Task Force** on Artificial Intelligence

2. **Regulatory Guidelines** for Use of Facial Recognition Technology

1.0 Task Force on Artificial Intelligence

Mission:

1. Oversee the **use of AI** within state government.
2. **Suggest legislation** around emerging AI technology.
3. Evaluate and **authorize new AI** technology.
    - Technical Advisory Committee*
4. Meets on a **quarterly** basis.

1.1 Task Force on Artificial Intelligence

Composition:

Chair & Vice Chair:
State Senator and State Representative

To include representatives from:

State Senate
State House of Representatives
Office of Information Technology
Impacted minority communities
Attorney General's office
Colorado State School Boards
State Board of Education

County Sheriffs of Colorado
Colorado Assn of Chiefs of Police
Colorado District Attorneys' Council
Statewide civil liberties advocacy org
Members of academia*
Members of industry*
Legal representatives*

***Technical Advisory Committee**

1.2 Task Force on Artificial Intelligence

Questions :

- Who is authorized to use a system?
- How will this use be regulated and overseen?
- Where and how are the data stored? For how long?
- Who must consent and how do they provide consent?
- What should the procurement process be for AI technology?
    - **OIT must establish standards for all departments to utilize for AI-related procurement.**

1.3 Task Force on Artificial Intelligence

Resources :

- Future of Privacy Forum AI & Ethics Resources
- Future of Privacy Forum Automated Decision-Making Systems: Considerations for State Policymakers
- NIST Proposal for Identifying and Managing Bias in AI
- GAO AI Accountability Framework
- FTC Best Practices for Common Uses of Facial Recognition Technologies
- And so many more...

2 Facial Recognition Policy Recommendations

- **No use in schools**
  - From preschool through higher education.
  - Protects the privacy and the civil liberties of some of our state's most vulnerable populations.
- **Minimum three-year moratorium** on investigatory use by law enforcement
  - Until the Technical Advisory Committee can evaluate use and provide recommendations.
  - Allows for use in redaction of video footage.
  - The data show that the risks of this emerging technology outweigh the potential benefits.

Expected Outcomes

More **intentional** use of **emerging** AI technology

Increased **security** of private data

Maintenance of **civil liberties** for both **minors** and adults

Avoidance of false arrests and
unnecessary encounters with law enforcement

It is not the responsibility of Colorado residents to fund the innovation of AI & facial recognition technology.

It is not the responsibility of Colorado residents to be guinea pigs for AI & facial recognition technology.

Acknowledgements

Sen. Chris Hansen
Sen. Bob Rankin
Sen. Robert Rodriguez
Sen. Janet Buckner
Rep. Brianna Titone
Rep. Alex Valdez
Rep. Mary Young

Dr. Brad Hayes
Dr. Casey Fiesler
Amie Stepanovich
Prof. Harry Surden
Jessica Finocchiaro
Aaquib Tabrez

Mark Ferrandino
Kate Sneed
Christina Van Winkle
Deb Thibault
Angela Kleis
Ted DeRosa
Russ Castagnaro

Matt Cagle
Denise Maes
Aly Schmidt
PJ Hoffman
Pamitha Weerasinghe

Jeff Riester
Sergeant Mike Honn
Chief Doreen Jokerst
Joel Malecka
Brandon Davis
Jery Payne
Michelle Zajic
Isabel Baird

Linda Kouskoutis
Hannah Nelson

Jesse Stricof
Jake Clark

Rock stars!

Thank You

Proposal Summary:

1. Task Force on AI
2. Facial recognition ban in schools, moratorium for law enforcement investigation

One Pager:

Other Issues of Interest:

- Data Privacy, including facial recognition implications
- Broadband Access & Affordability
- Right to Repair
- Other issues related to AI and technology

Please contact me:
christine.chang@colorado.edu
206.330.6729

Appendix / Backup

What will this cost?

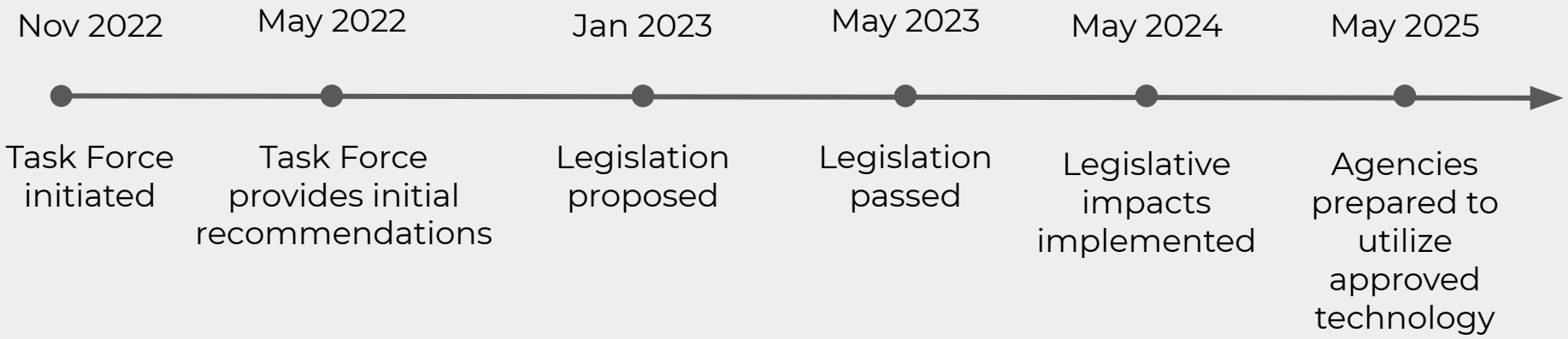
Task Force:

- 0.4 FTE for LCS & OLLS support
- Other members participate as part of their normal job tasks or on a volunteer basis (academia, industry)

Legislation:

- 0.4 FTE for LCS support
- Other costs minimal

Why a three-year moratorium?



* Not to scale

Why ban facial recognition in schools?

- The technology does not work as well on children.
- Schools are places where students should be safe, and research shows that students feel less safe when surrounded by technology like metal detectors and surveillance cameras.
- PreK-12 students are not old enough to provide consent.
- Most school shootings are committed by people who are supposed to be in the building.

Facial Recognition Software Will Not Stop School Shootings

https://slate.com/technology/2018/05/locksport-school-districts-facial-recognition-software-will-not-stop-a-mass-shooting.html