FUTURE OF PRIVACY FORUM

Biometrics: Law and Public Policy

Washington Privacy Week

January 2025

Tatiana Rice

Director, U.S. AI Legislation

Future of Privacy Forum

FPF MEMBERS & TEAM

200+ Companies

45+ Academics

20+ Civil Society

4 Global Offices

- Washington, DC
- Brussels
- Singapore
- Tel Aviv

Presentation GOALS

- **How biometric systems work**, including definitions, technology processes, and differences among common systems;

- **The benefits and risks**, including efficiencies, potential harms, and privacy and bias considerations; and

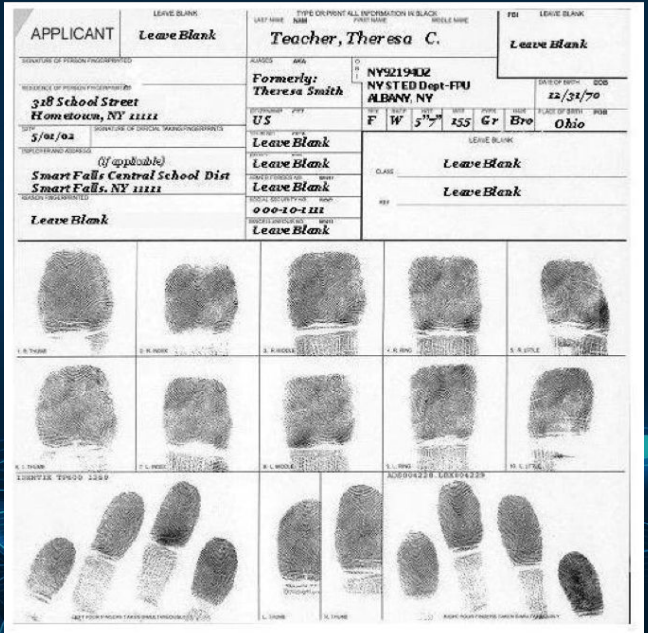
- **Regulatory perspectives,** including U.S. federal and state biometrics and AI regimes.

AGENDA

1. Explanation of Biometric Identification and Verification
2. Risks and Benefits
3. Regulatory Approaches
4. Takeaways

Biometric Identification & Verification

- How humans identify each other
  - Face, Voice, Mannerisms
- FBI Fingerprint Repository begun in 1924
- Focus is on **<u>identity</u>** – how can devices tell people apart?
- Identity paradigms:
  - What you know (password, passkey)
  - What you have (key card, license)
  - **<u>Who you are</u>**
    - Biometric recognition is "automated recognition of <u>individuals</u> based on their <u>behavioral</u> and <u>biological</u> characteristics"



APPLICANT

LEAVE BLANK
Leave Blank

TYPE OR PRINT ALL INFORMATION IN BLACK
Teacher, Theresa C.

FBI LEAVE BLANK
Leave Blank

ALIASES AKA
Formerly:
Theresa Smith

NY921940Z
NYSTED Dept-FPU
ALBANY, NY

DATE OF BIRTH DOB
12/31/70

318 School Street
Hometown, NY 11111

US

F	W	5"7"	155	Gr	Bro

PLACE OF BIRTH POB
Ohio

5/01/02

Leave Blank

(If applicable)
Smart Falls Central School Dist
Smart Falls. NY 11111

Leave Blank

LEAVE BLANK
CLASS Leave Blank
REF Leave Blank

Leave Blank

000-10-1111

Leave Blank

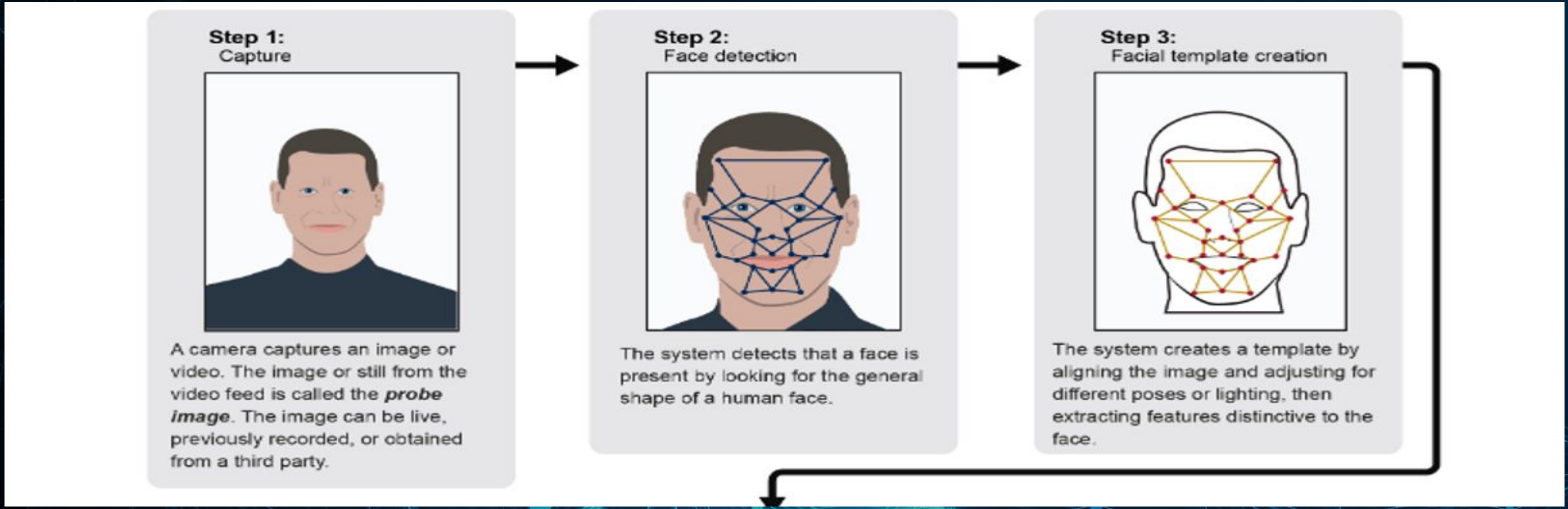
Leave Blank

Commercial Use Cases

- **Why use automated recognition systems?**
  - Scale
  - Accuracy
  - Reliability
  - Human Fallibility

- **Common Modalities**
  - Face
  - Finger
  - Iris
  - Voice
  - Behavioral (gait, keystroke, eye-tracking)

Identification & Verification



Step 1: Capture

A camera captures an image or video. The image or still from the video feed is called the ***probe image***. The image can be live, previously recorded, or obtained from a third party.

Step 2: Face detection

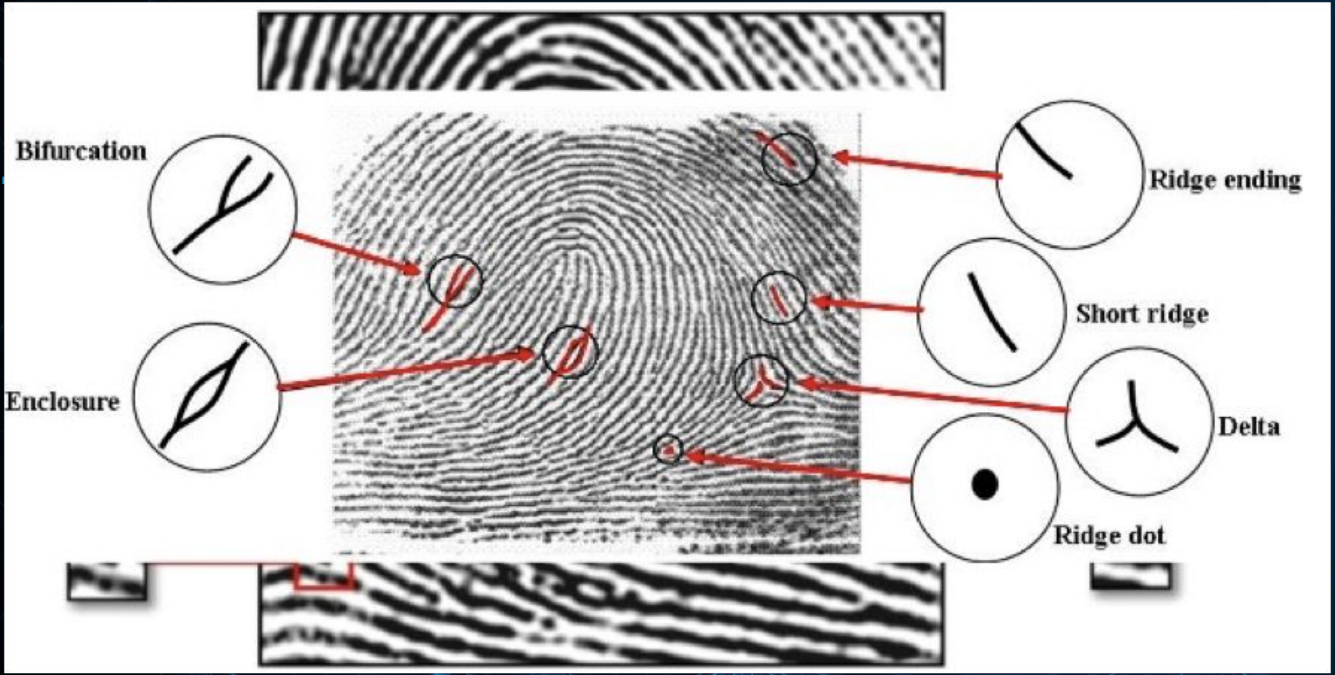
The system detects that a face is present by looking for the general shape of a human face.

Step 3: Facial template creation

The system creates a template by aligning the image and adjusting for different poses or lighting, then extracting features distinctive to the face.

Face recognition

- One of the most common modalities of biometric systems
- Based on distances & ratios between facial points
- High-end systems use up to 1,000 different vectors to create a "template"



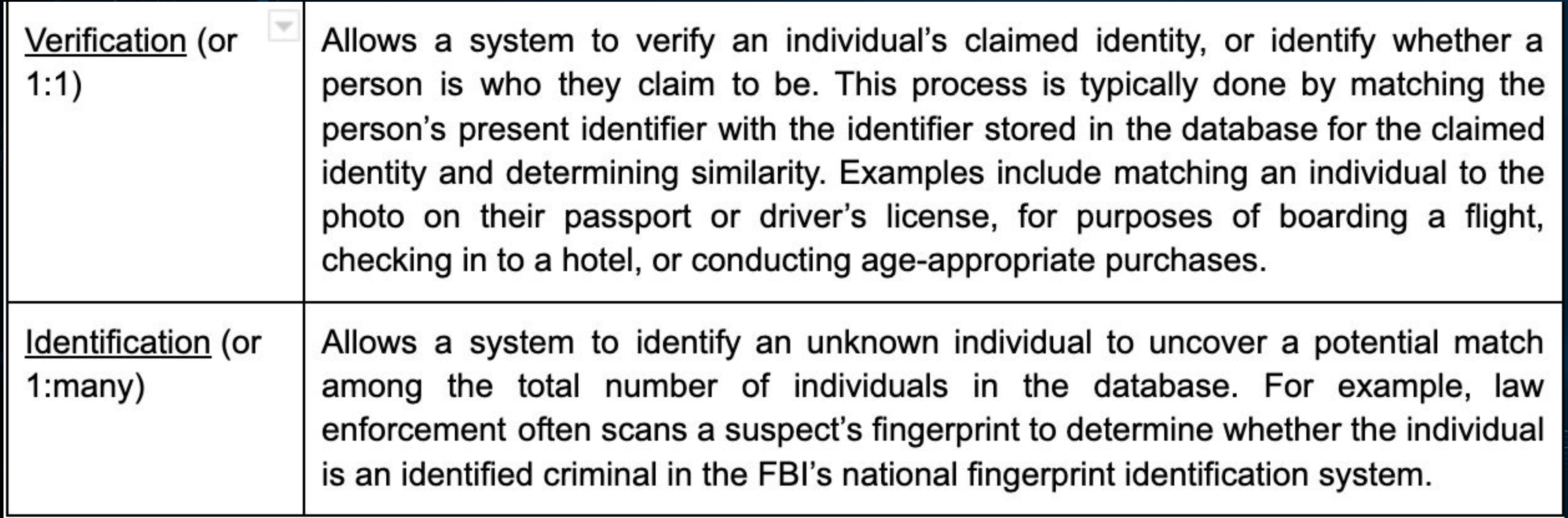
Fingerprint Recognition

- Fingerprint templates store type, size, and orientation of minutia points, relative to the core

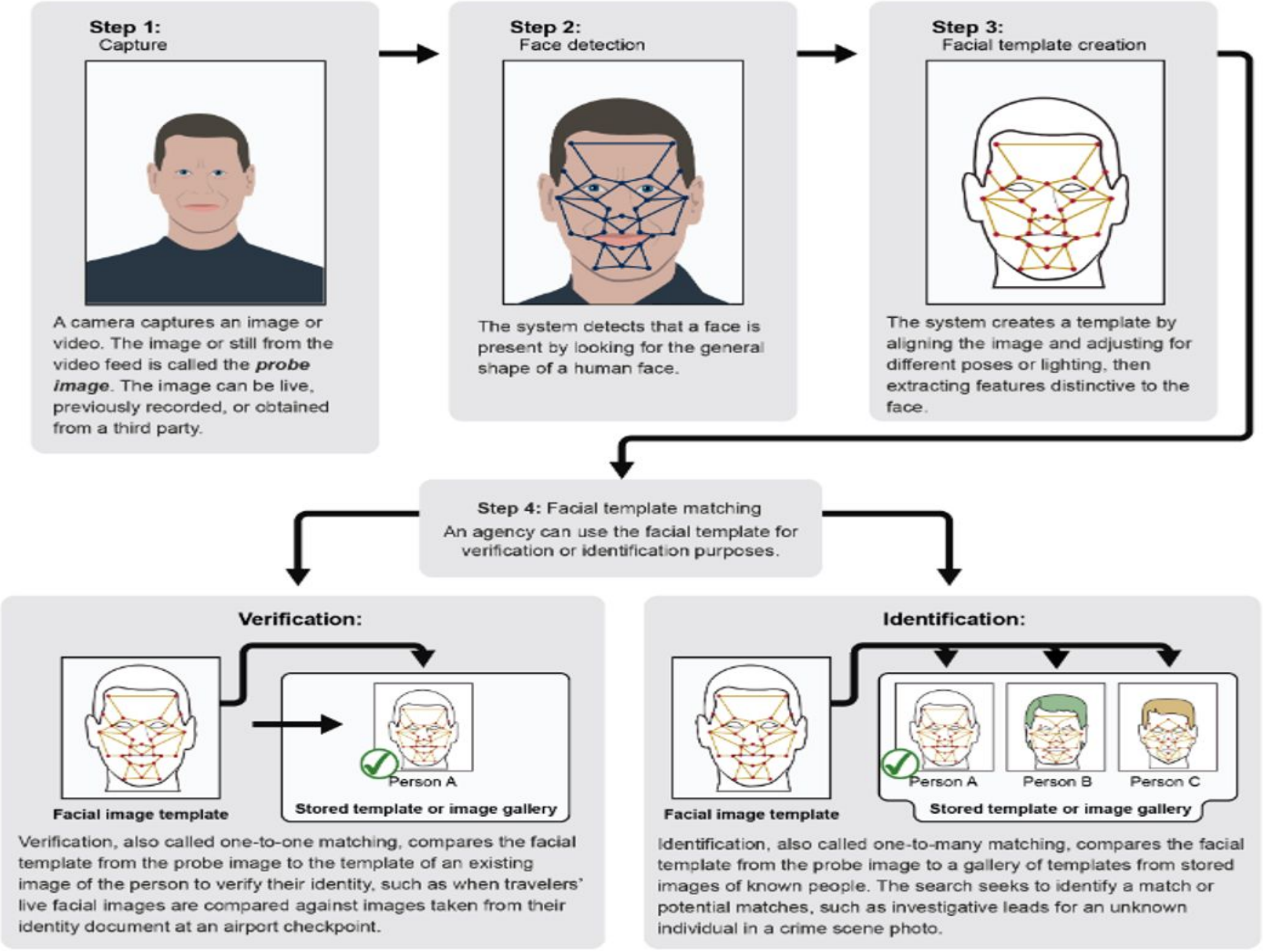
Common Commercial Use Cases

- Employee or consumer identity verification
  - Access management
    - Physical facility
    - Personal or business device
    - Account
    - Proprietary system or database
- Retail theft prevention
  - Post-incident software
  - Ongoing monitoring

Identification v. Verification: There's a Difference



Verification (or 1:1)	Allows a system to verify an individual's claimed identity, or identify whether a person is who they claim to be. This process is typically done by matching the person's present identifier with the identifier stored in the database for the claimed identity and determining similarity. Examples include matching an individual to the photo on their passport or driver's license, for purposes of boarding a flight, checking in to a hotel, or conducting age-appropriate purchases.
Identification (or 1:many)	Allows a system to identify an unknown individual to uncover a potential match among the total number of individuals in the database. For example, law enforcement often scans a suspect's fingerprint to determine whether the individual is an identified criminal in the FBI's national fingerprint identification system.



Step 1: Capture

A camera captures an image or video. The image or still from the video feed is called the ***probe image***. The image can be live, previously recorded, or obtained from a third party.

Step 2: Face detection

The system detects that a face is present by looking for the general shape of a human face.

Step 3: Facial template creation

The system creates a template by aligning the image and adjusting for different poses or lighting, then extracting features distinctive to the face.

Step 4: Facial template matching

An agency can use the facial template for verification or identification purposes.

Verification:

Verification, also called one-to-one matching, compares the facial template from the probe image to the template of an existing image of the person to verify their identity, such as when travelers' live facial images are compared against images taken from their identity document at an airport checkpoint.

Identification:

Identification, also called one-to-many matching, compares the facial template from the probe image to a gallery of templates from stored images of known people. The search seeks to identify a match or potential matches, such as investigative leads for an unknown individual in a crime scene photo.

Source: GAO analysis. | GAO-22-106100

AGENDA

1. Explanation of Biometric Identification and Verification
2. Risks and Benefits
3. Regulatory Approaches
4. Takeaways

Potential Risks

- Privacy/security
- Risk of bias/inaccuracy

Why is Biometric Data is High-Risk for Privacy and Security?

FUTURE OF PRIVACY FORUM

- ***Immutability*** - Unlike financial information or social security numbers, biometric templates typically cannot be changed. Therefore, if compromised by a bad actor, there is minimal to no recourse for a consumer.
    - However, considerations for advanced proprietary encryption software
- ***Deepfakes & Access*** - biometric data is commonly used to access other sensitive information, devices, or facilities–increasing the risk of concerted identity theft.
- ***Surveillance*** - identification systems used to surveil society or specific individuals can cause a "chilling effect" on the speech and activities of individuals

Accuracy of Biometric Recognition

- Biometric systems can fail in multiple ways…blurry iris, low lighting in photos, smudged print.

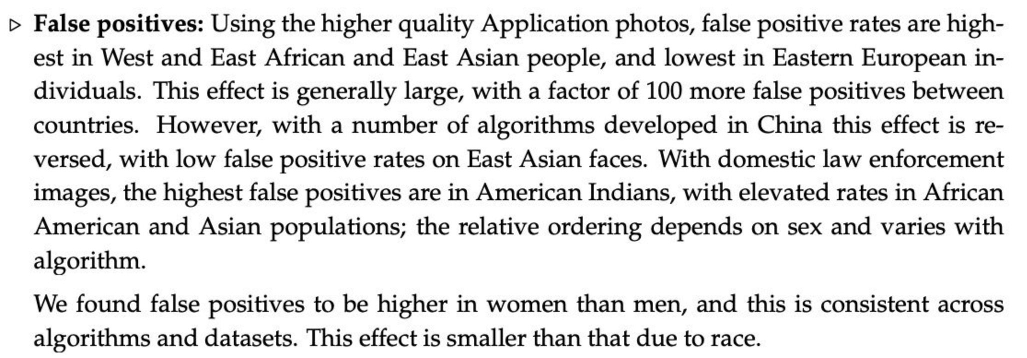
- Types of Algorithm Errors
  - False positive
  - False negative

		The Real World	
		Same Person (Mate)	Not (Non-mate)
Algorithm Says	Match	True Match	False Match
	Non-match	False Non-match	True Non-match

$$Accuracy = \frac{Number\ of\ Correct\ Predictions}{Total\ Number\ of\ Predictions}$$

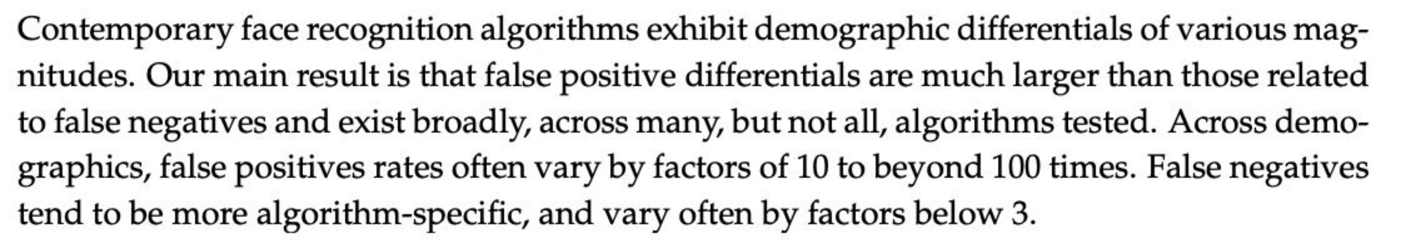
NIST Testing of Accuracy & Bias

- NIST 2019 “Demographic Differentials” Testing
  - *“While it is usually incorrect to make statements across algorithms, we found empirical evidence for the existence of demographic differentials in the majority of the face recognition algorithms we studied,” said Patrick Grother, a NIST computer scientist and the report’s primary author.”*



▷ **False positives:** Using the higher quality Application photos, false positive rates are highest in West and East African and East Asian people, and lowest in Eastern European individuals. This effect is generally large, with a factor of 100 more false positives between countries. However, with a number of algorithms developed in China this effect is reversed, with low false positive rates on East Asian faces. With domestic law enforcement images, the highest false positives are in American Indians, with elevated rates in African American and Asian populations; the relative ordering depends on sex and varies with algorithm.

We found false positives to be higher in women than men, and this is consistent across algorithms and datasets. This effect is smaller than that due to race.



Contemporary face recognition algorithms exhibit demographic differentials of various magnitudes. Our main result is that false positive differentials are much larger than those related to false negatives and exist broadly, across many, but not all, algorithms tested. Across demographics, false positives rates often vary by factors of 10 to beyond 100 times. False negatives tend to be more algorithm-specific, and vary often by factors below 3.

Example: Comparative Demographic Differential Testing

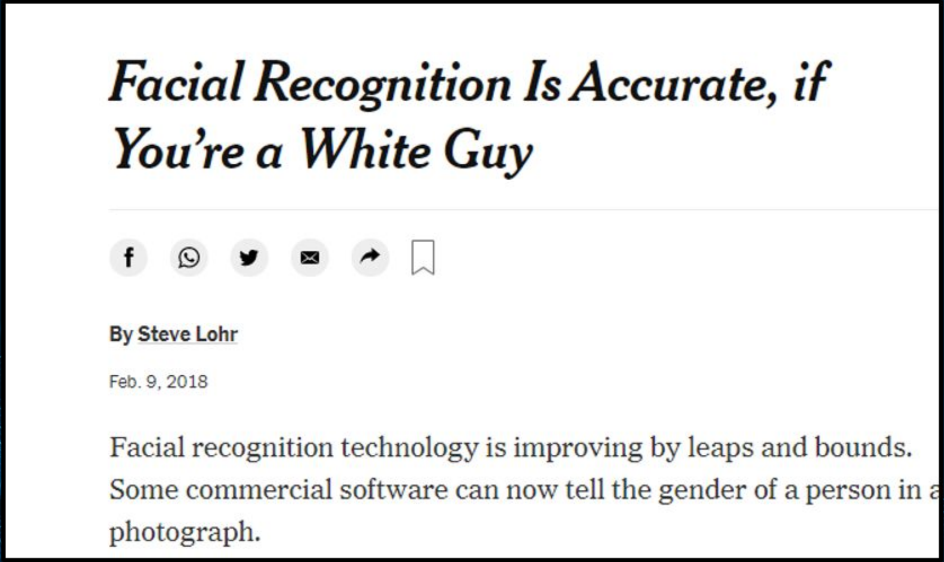
Performance and Error Rates

- E. Asian faces experience 644% of the false positive rate that White faces experience.

Demographic Groups	Acc. Ratio	TPR Ratio	FPR Ratio	TNR Ratio	FNR Ratio
E. Asian-to-White	1.005	1.012	6.438	0.973	0.394
Black-to-White	0.969	0.951	0.000	1.005	3.488
S. Asian-to-White	1.017	1.020	0.000	1.005	0.000
Female-to-Male	0.988	0.987	#DIV/0!	0.992	2.276

How Bias Arises

- Lack of representative training data ("garbage in, garbage out")
- Homogenous engineers/perspectives
- Biased design choices made by model or engineer
- Biased application (targeting certain populations)



Facial Recognition Is Accurate, if You're a White Guy

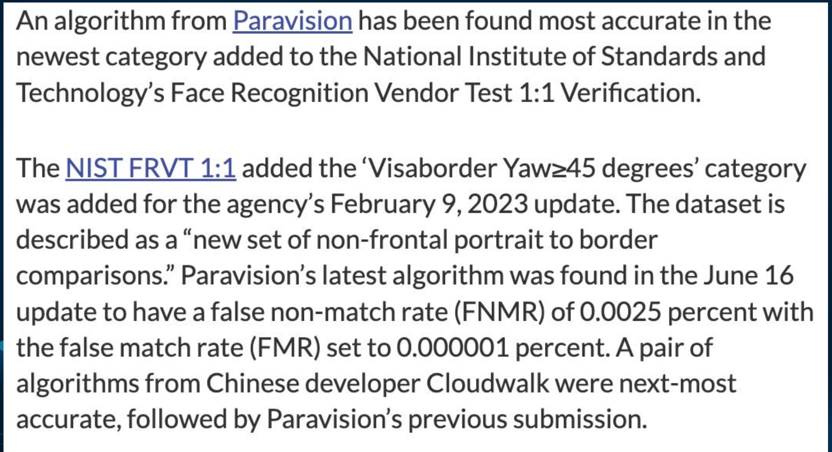
By Steve Lohr

Feb. 9, 2018

Facial recognition technology is improving by leaps and bounds. Some commercial software can now tell the gender of a person in a photograph.

NIST Testing of Accuracy & Bias

- **But FVRT accuracy across demographic differentials has significantly improved since 2019.**



An algorithm from Paravision has been found most accurate in the newest category added to the National Institute of Standards and Technology's Face Recognition Vendor Test 1:1 Verification.

The NIST FRVT 1:1 added the 'Visaborder Yaw≥45 degrees' category was added for the agency's February 9, 2023 update. The dataset is described as a "new set of non-frontal portrait to border comparisons." Paravision's latest algorithm was found in the June 16 update to have a false non-match rate (FNMR) of 0.0025 percent with the false match rate (FMR) set to 0.000001 percent. A pair of algorithms from Chinese developer Cloudwalk were next-most accurate, followed by Paravision's previous submission.

"The major result in NIST IR 8271 was that ***massive gains in accuracy have been achieved****...and these far exceed improvements made in the prior period. While the industry gains were broad -* ***at least 30 developers' algorithms outperformed the most accurate algorithm from late 2013, there remains a wide range of capability...the most accurate algorithm reported here is substantially more accurate than anything reported in NIST IR 8271.***

Harms are Often Concentrated on Marginalized Groups

- **“High-Risk” Contexts**
    - Law enforcement and immigration enforcement
    - Fraud detection systems
    - “Landlord tech”
    - Access to benefits
    - Access to finances

So Why Use Biometric Data At All?

- ***More accurate and scalable than human eye***

- ***Security*** - One of the strongest methods of security for governments, consumers, and businesses, particularly when used with MFA.
  - It is far more robust and difficult to crack than other authentication methods such as username-password combinations or identification cards.

- ***Fraud Detection*** - biometrics are non-transferable, making it more difficult for employees to fraudulently provide credentials to other employees or bad actors

- ***Often required by Law*** - background checks, "reasonable security."

- ***Convenience***

AGENDA

1. Explanation of Biometric Identification and Verification
2. Risks and Benefits
3. Regulatory Approaches
4. Takeaways

AGENDA

Regulatory Approaches

1. Biometric Data Privacy Laws
2. BIPA Litigation
3. Comprehensive Data Privacy Laws
4. AI Regulations

Biometric Data Privacy Laws

- ***Definitions***: largely limit the scope of “biometric information” or “biometric data” to data collected for purposes related to identification, with some exceptions (including Texas, and emerging case law in Illinois)

- **WASHINGTON Chapter 19.375 RCW:**
  - **"Biometric system"** means an automated identification system capable of capturing, processing, and storing a biometric identifier, comparing the biometric identifier to one or more references, and matching the biometric identifier to a specific individual.
  - "**Biometric identifier**" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual.

Biometric Data Privacy Laws

FUTURE OF PRIVACY FORUM

	Illinois BIPA	Texas CUBI	Washington
Covers:	Biometric Identifiers Biometric Information	Biometric Identifiers	Biometrics Identifiers Biometric Systems
Requirements:	● Publicly available destruction/retention schedule ● Notice and consent ● No sale/share ● Reasonable Security	● Notice and consent ● No sale/share ● Destruction schedule ● Reasonable Security	● Notice and consent ● No sale/share ● Reasonable Security ● Retention schedule UNLESS for a "security purpose"
Enforcement:	PRA, AG	AG	AG

Affirmative Consent is a Must

Obtain express, affirmative consent when:

1. Enrolling an individual in a program that uses biometric recognition technology for verification or identification purposes; and/or
2. Identifying an individual to third parties who would not otherwise have known that individual's identity.

WA: "(2) Notice is a <u>disclosure, that is not considered affirmative consent</u>, that is given through a procedure reasonably designed to be readily available to affected individuals. The exact notice and type of consent…is context-dependent."

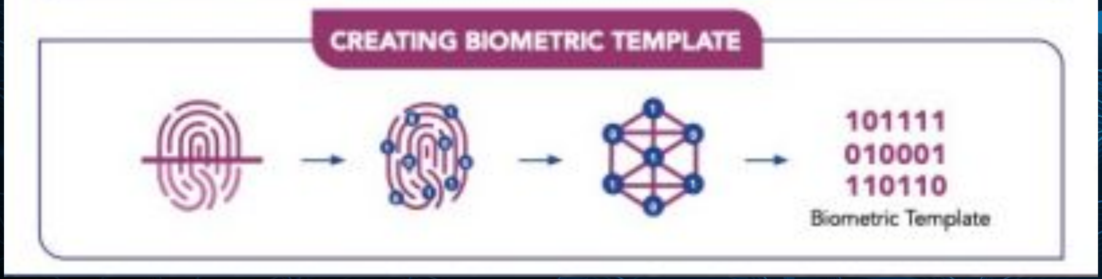
Some Exemptions (depending on law)**:**

- Collections of data for physical security, fraud, and asset protection programs
- When sharing occurs within a vendor management framework, where the third party is a contracted services partner necessary to provide the good or service requested by the individual, and who is bound by the same controls.

Reasonable Security

Companies must maintain a comprehensive data security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of personal information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.

Most common and secure method is "biometric encryption" or "biometric hashing"



Data Minimization & Policies

- Data is only stored as long as reasonably necessary for the processing purpose.
  - BIPA requires at minimum after 3 years
- Business has a policy that explains to the individual to whom data is being collected:
  - The purpose of the collection;
  - The length of time the data will be stored, and when it will be deleted;
  - Any rights provided by the law;
  - Any alternatives (EU General Data Protection Regulation);

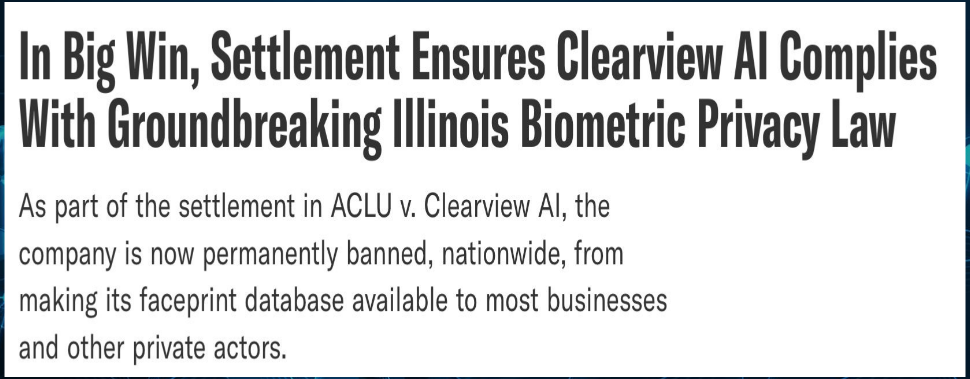
ACLU Model Biometric Law

- Consumer right of access
- Consumer right of deletion

BIPA Litigation

How U.S. policymakers, advocates, and the courts have thought about the scope of these laws is heavily dependent on the Illinois Biometric Privacy Act (BIPA). BIPA's private right of action has allowed courts to decide the boundaries of what technologies should and should not be within the scope of biometrics law.

It has also fundamentally changed how businesses think about collecting and managing biometric data.

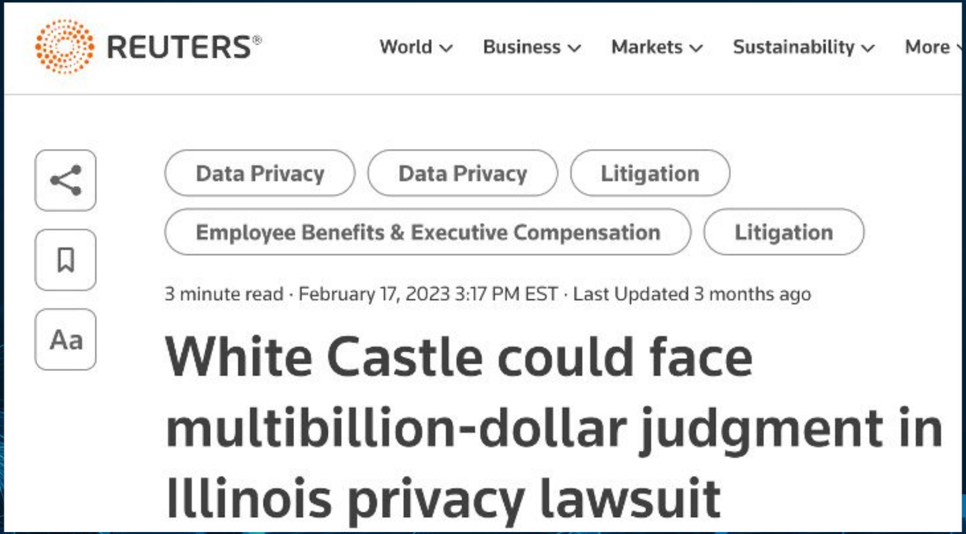


In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law

As part of the settlement in ACLU v. Clearview AI, the company is now permanently banned, nationwide, from making its faceprint database available to most businesses and other private actors.

BIPA Litigation

- Over 2,000 class action lawsuits in Illinois. Heavy incentives for businesses to settle before trial.
- No injury requirement, statutory damages
- First jury trial award of $428 million
- 5-year statute of limitations
- Per-scan violations
- No retroactive compliance measures



Data Privacy Data Privacy Litigation

Employee Benefits & Executive Compensation Litigation

3 minute read · February 17, 2023 3:17 PM EST · Last Updated 3 months ago

White Castle could face multibillion-dollar judgment in Illinois privacy lawsuit

BIPA Litigation: Key Issue Areas

FUTURE OF PRIVACY FORUM

- ***Photos Might be Biometrics When "Biometric Templates" are Extracted***

- ***What is the difference between a voice print and voice recording?***

- ***Possession and Collection:*** When is an entity in "possession" of biometrics? On-device storage versus storage on servers.

- ***Coverage of Third-Party Vendors:*** Generally BIPA Applies to Biometrics Technology Providers & Third-Party Vendors.

Comprehensive Data Privacy Laws

19(?) Comprehensive Privacy Laws: California, Colorado, Connecticut, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Virginia, Utah

Biometric Data is considered a "sensitive category" of personal information. These laws have the following requirements for sensitive data:

- Consumer consent for processing
- Data protection assessment
- Right to opt-out of processing (California)

Other Approaches

California: Prohibits employers from requiring an employee to be fingerprinted or photographed as a condition of employment if the employer plans to provide the information to a third party and if the information could be used to the employee's detriment. (California Labor Code §1051)

Florida: bars public schools from collecting, obtaining or retaining any biometric information from students or their immediate family members. (Fla. Stat. § 1002.222(1)(a))

New York:

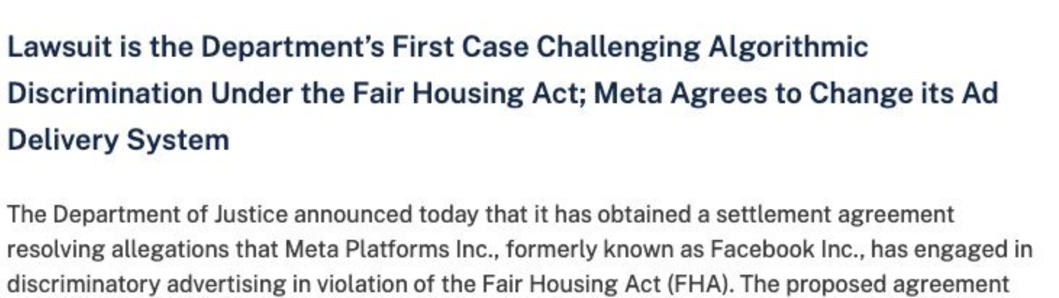
- Prohibits the use of biometric identifying technology in schools (Sec. 106-B)
- Prohibits employers from fingerprinting employees as a condition of employment unless specifically authorized by another law (N.Y. Labor Law § 201-a)
- Requires notice of collection practices in NYC (NYC Admin. Code §§ 22-1201 – 1205)

Portland, OR: bans facial recognition technology by all public and private entities (Ch. 34.10)

- 17 other municipalities have banned government use of facial recognition

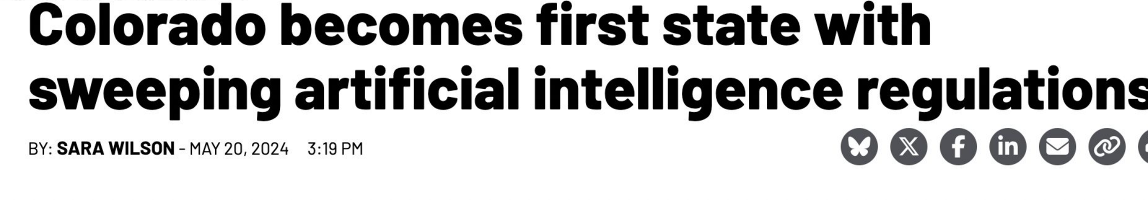
AI Regulations Apply to Biometric Systems

- **Civil Rights laws already apply to areas/tasks conducted by AI** (ex: housing, employment, consumer finance, credit, etc.)
- **Colorado AI Act and Other High-Risk AI Legislation**
- **FTC and UDAP Enforcement**
- **EU AI Act:** a broad risk-based approach to AI regulation.
  - Unacceptable risk, high-risk, limited risk, and minimal risk
  - Differing requirements/limitations based on risk profile



Lawsuit is the Department's First Case Challenging Algorithmic Discrimination Under the Fair Housing Act; Meta Agrees to Change its Ad Delivery System

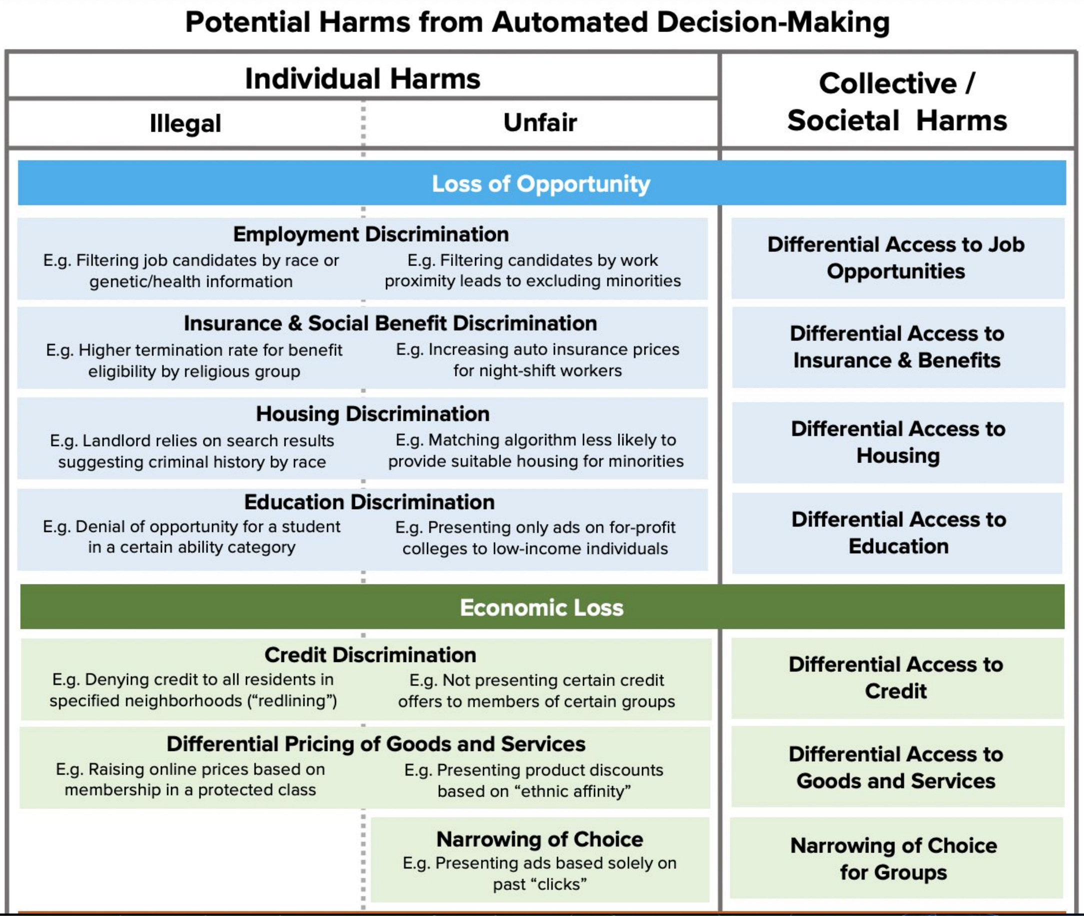
The Department of Justice announced today that it has obtained a settlement agreement resolving allegations that Meta Platforms Inc., formerly known as Facebook Inc., has engaged in discriminatory advertising in violation of the Fair Housing Act (FHA). The proposed agreement



Colorado becomes first state with sweeping artificial intelligence regulations

BY: **SARA WILSON** - MAY 20, 2024 3:19 PM

A key goal for many lawmakers is to mitigate the risk of algorithmic discrimination



Potential Harms from Automated Decision-Making

Individual Harms		Collective / Societal Harms
Illegal	Unfair	
Loss of Opportunity		
Employment Discrimination E.g. Filtering job candidates by race or genetic/health information	E.g. Filtering candidates by work proximity leads to excluding minorities	Differential Access to Job Opportunities
Insurance & Social Benefit Discrimination E.g. Higher termination rate for benefit eligibility by religious group	E.g. Increasing auto insurance prices for night-shift workers	Differential Access to Insurance & Benefits
Housing Discrimination E.g. Landlord relies on search results suggesting criminal history by race	E.g. Matching algorithm less likely to provide suitable housing for minorities	Differential Access to Housing
Education Discrimination E.g. Denial of opportunity for a student in a certain ability category	E.g. Presenting only ads on for-profit colleges to low-income individuals	Differential Access to Education
Economic Loss		
Credit Discrimination E.g. Denying credit to all residents in specified neighborhoods ("redlining")	E.g. Not presenting certain credit offers to members of certain groups	Differential Access to Credit
Differential Pricing of Goods and Services E.g. Raising online prices based on membership in a protected class	E.g. Presenting product discounts based on "ethnic affinity"	Differential Access to Goods and Services
	Narrowing of Choice E.g. Presenting ads based solely on past "clicks"	Narrowing of Choice for Groups

Evidence of discrimination occurring due to AI biases and inaccuracies is well-documented and prevalent.

Civil Rights

What is Legal Discrimination? How to Apply to AI?

Employment Example: (from EEOC Uniform Guidelines)

- Title VII prevents employers from using tests or selection methods that, despite appearing neutral, unfairly disadvantage people, known as "**disparate impact**" "**adverse impact,**" occurs when the procedures used aren't essential to the job's performance.

- **Four-Fifths Rule:** If the selection rate for a protected group is less than 80% of the selection rate for the group with the highest selection rate, it may indicate an adverse impact.

Why State Lawmakers Looked to Regulate

- **Protecting Privacy and Data Security:** AI relies on vast amounts of personal data, creating a heightened risk of privacy breaches. Lawmakers aim to ensure that AI systems handle personal information securely and transparently, protecting citizens' privacy rights.
- **Ensuring Fairness and Preventing Discrimination:** AI systems can unintentionally perpetuate biases present in their training data, leading to discriminatory outcomes. Regulations aim to ensure that AI systems are fair, equitable, and do not discriminate against individuals based on race, gender, or other protected characteristics.
- **Enhancing Transparency and Accountability:** AI decision-making processes can often be opaque, making it difficult for individuals to understand how decisions that affect them are made. Regulations seek to enhance transparency, ensuring that AI systems are accountable and that their decision-making processes can be scrutinized and understood.

- **Promoting Ethical AI Development and Use:** State lawmakers aim to establish ethical guidelines for the development and use of AI to ensure that these technologies are aligned with societal values and public interest.
- **Supporting Innovation and Competitiveness:** By providing clear regulatory frameworks, states can foster a stable environment for AI innovation. This can attract investment and talent, helping states remain competitive in the rapidly evolving tech landscape.
- **Addressing Safety and Security Concerns:** AI systems, particularly those used in critical infrastructure, healthcare, transportation, and law enforcement, must be reliable and secure. Regulations aim to ensure that these systems are safe and do not pose

Colorado AI Act: Scope and Regulated Entities

Developers and **Deployers** (doing business in Colorado) of “**High-Risk AI Systems**”

1. **“High Risk AI System”**
   - **a.** *Any **artificial intelligence system**;*
   - **b.** *That when deployed, makes, or is a **substantial factor** in making;*
   - **c.** *A **consequential decision**. (Sec. 6-1-1701(9(a)).*

2. **Regulated Entities**
   - a. “Developer”
   - b. “Deployer”

3. **Carve-Outs or Exceptions**

SB 24-205: Scope and Regulated Entities

Types of Technologies: “High Risk AI System”

“High Risk AI System”

1. *Any **artificial intelligence system**;*
2. *That when deployed, makes, or is a **substantial factor** in making;*
3. *A **consequential decision**. (Sec. 6-1-1701(9(a)).*

“Consequential Decision”: *Any decision that:*

1. *Has a **material, legal or similarly significant effect**;*
2. *On the **provision or denial** to any consumer of, or the cost or terms of:*
3. *Areas: (A) Education; (B) Employment; (C) Financial or lending services; (D) Essential government services; (E) Healthcare service; (F) Housing, (G) Insurance, or (H) Legal services. (Sec. 6-1-1701(3)).*

Duty of Care: Algorithmic Discrimination

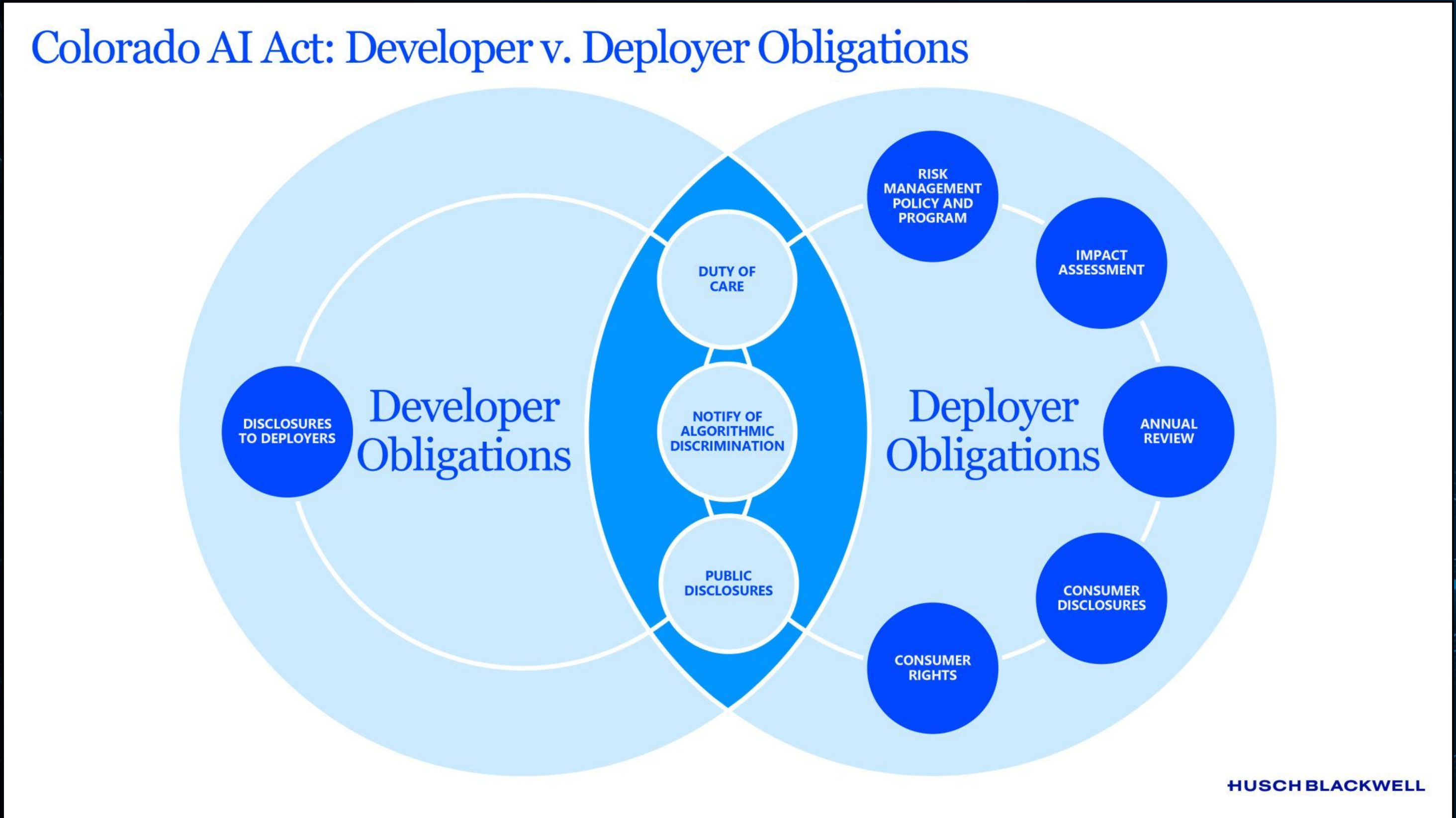
Algorithmic Discrimination: Any condition where the use of an AI system **results in unlawful differential treatment or impact** that disfavors an individual or group of individuals based on their protected class. (Sec. 6-1-1701(1)(a)).

- **EXCLUDES**: self-testing to mitigate or prevent discrimination or otherwise ensure compliance with state or federal law, expanding customer or applicant pool, private clubs.

Duty to Avoid Algorithmic Discrimination: Developers and Deployers shall use **reasonable care** to protect consumers from any **known or reasonably foreseeable** risk of algorithmic discrimination arising from the **intended and contracted use** of the high-risk AI system.

Developers and deployers maintain a rebuttable presumption of using reasonable care under this provision if they satisfy the obligations of the Act.

Developer and Deployer Obligations



Colorado AI Act: Developer v. Deployer Obligations

Developer Obligations

DISCLOSURES TO DEPLOYERS

DUTY OF CARE

NOTIFY OF ALGORITHMIC DISCRIMINATION

PUBLIC DISCLOSURES

Deployer Obligations

RISK MANAGEMENT POLICY AND PROGRAM

IMPACT ASSESSMENT

ANNUAL REVIEW

CONSUMER DISCLOSURES

CONSUMER RIGHTS

HUSCH BLACKWELL

The Technology-Specific Approach: Generative AI

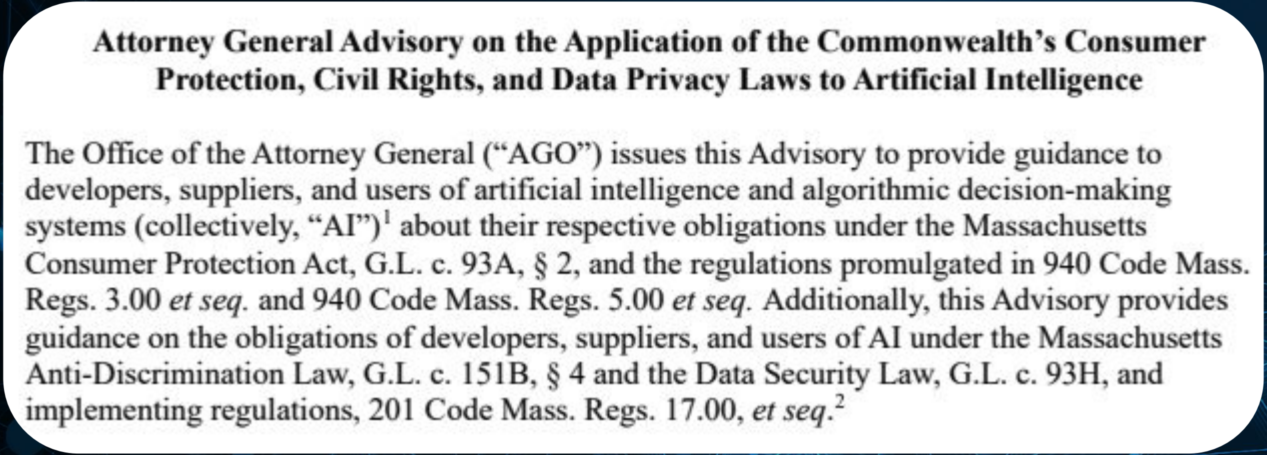
Focus: Enhancing Transparency about Generative AI inputs, use, and outputs

- **Utah SB 149 (Enacted):** Requiring individuals or entities to clearly and conspicuously disclose when a generative AI system is interacting with a consumer in certain consumer contexts protected by UDAP
- **California**
  - 2018 law that prohibits using a "bot" to communicate or interact with the intent to mislead individuals about the bot's artificial identity
  - **AB 2013**: Mandates that developers of generative AI systems publicly disclose documentation about the **data** used to train these systems.
    - Biometric implications

  SB 942 : Requires entities providing generative AI tools to offer an "**AI detection tool**" that lets individuals check whether content was created or modified by the AI system

Consumer Protection

- **Section 5:** FTC can investigate and enforce against "unfair and deceptive" trade practices
    - Similar state-level regimes for state Attorneys General



Attorney General Advisory on the Application of the Commonwealth's Consumer Protection, Civil Rights, and Data Privacy Laws to Artificial Intelligence

The Office of the Attorney General ("AGO") issues this Advisory to provide guidance to developers, suppliers, and users of artificial intelligence and algorithmic decision-making systems (collectively, "AI")[1] about their respective obligations under the Massachusetts Consumer Protection Act, G.L. c. 93A, § 2, and the regulations promulgated in 940 Code Mass. Regs. 3.00 *et seq.* and 940 Code Mass. Regs. 5.00 *et seq.* Additionally, this Advisory provides guidance on the obligations of developers, suppliers, and users of AI under the Massachusetts Anti-Discrimination Law, G.L. c. 151B, § 4 and the Data Security Law, G.L. c. 93H, and implementing regulations, 201 Code Mass. Regs. 17.00, *et seq.*[2]

Consumer Protection - FTC Action Against Rite Aid for Unfair Use of Facial Recognition Showcases Need for Internal AI Governance

- Case involving company use of FRT purchased from vendors for anti-theft. Lack of AI governance resulted in thousands of FRT false positive match alerts, with a notable error rate for people of color and women. Individuals were falsely accused, reported, and placed in detention.
- **FTC determined unfair trade practice:** failure to assess accuracy and mitigate bias, use of low-quality images, lack of monitoring or oversight
- Required model disgorgement
- This is the first time the Commission has used its Section 5 unfairness authority to address algorithmic discrimination.

Consumer Protection - FTC Action Against Rite Aid for Unfair Use of Facial Recognition Showcases Need for Internal AI Governance

Takeaways

- It is not enough to simply deploy AI products from vendors; AI deployers should be creating and maintaining an enforceable AI governance program that incorporates:
  - accuracy and bias testing
  - data quality assessments
  - human training and oversight.

- Measures taken to identify and mitigate algorithmic bias should address the entirety of the AI lifecycle.

Federal Trade Commission

The FTC is actively leaning on its existing Section 5 authority, and in some cases seeking to expand it.

AI-Related Guidance / Enforcement (ex: Rite-Aid)

- Watch for discriminatory outcomes
- Embrace transparency
- Provide understandable disclosures about how data is used
- Keep your AI claims in check
- Don’t exaggerate capability of product
- Have evidence to support claims relating to performance of AI
- Make it clear to consumers whether content is “real” and reflects a commercial relationship with a known person or entity, or the product of AI

AGENDA

1. Explanation of Biometric Identification and Verification
2. Risks and Benefits
3. Regulatory Approaches
4. Takeaways

Main Takeaways

I. **Biometrics technologies range widely in purpose and risk profile (including 1:1, 1:Many, characterization, and detection).**

   A. Identification and Authentication systems are essential to many businesses’ and consumers’ security.

   B. Identification and Authentication systems have unique high privacy and security risks.

   C. All systems pose a risk of bias and discrimination

Main Takeaways

I. **Most U.S. biometric privacy laws are fairly consistent:**
   A. Biometrics are used for identification/authentication of identity
   B. Affirmative consent is required
   C. Data should be retained only as necessary and deleted as soon as practical
   D. There should be reasonable security

II. **BIPA litigation is driving most biometric privacy compliance and policy developments:**
   A. More businesses are treating biometric data with heightened sensitivity
   B. The breadth of technologies affected is expanding, including those unrelated to the identification/authentication of individual identity

Main Takeaways

III. AI regulations focused on bias, transparency, and consumer protection apply to biometrics used, particularly in high-risk scenarios against individuals

A. Transparency and mitigation for biometrics used for AI training

B. Internal AI governance

C. Risk assessments

D. Employee training and oversight

E. Due diligence w/ vendors

FUTURE OF PRIVACY FORUM

QUESTIONS?

Tatiana Rice

trice@fpf.org

@futureofprivacy

Headshot