ACLU Colorado

Privacy and Liberty

2024 Mini-report

Corporations have nearly unlimited power to collect, store, buy and sell an individual's unique biometric data, including information about one's DNA, facial mapping and fingerprints.

The Colorado Biometric Identifiers Privacy Act (BIPA) would **strengthen transparency and reduce the risk of misuse, nonconsensual sharing and exploitation of that data.**

What is biometric data?

Biometric data is any information that consists of one or more biological, physiological or behavioral characteristics that can be used (alone or in combination with other information) to identify an individual. This includes fingerprints, voiceprints, DNA sequences, facial characteristics and handwriting.

Why is protecting biometric data important?

Biometric data is especially sensitive.

Biometric data can reveal intimate details about a person's life, such as the likelihood they will contract certain diseases. When this personal data is shared, it could lead to adverse outcomes such as higher insurance premiums and denial of life insurance.

There are risks even when biometrics are used knowingly and consensually. Increasingly, biometric data is being used for security purposes, like using a fingerprint or faceprint as a password. Using information in this way poses unique challenges; for example, biometric identifiers cannot be changed in the event of a security breach.

Certain biometric technologies have higher failure rates based on race, gender, and age, but all people are at risk of false matches.

Facial recognition software has significantly higher failure rates when it comes to identifying Indigenous people, People of Color, women, youth and older adults. According to a 2019 study led by the U.S. government's National Institute of Standards and Technology, many facial recognition algorithms were far more likely to misidentify non-white people.[1]

Because of these failure rates, some law enforcement police searches that have relied on facial recognition technology have led to false arrests. The vast majority of these false arrests have involved Black people.

Some algorithms were found to be up to **100 times more likely to misidentify non-white people.** Native American, Black and Asian people are all disproportionately more likely to be misidentified.

Source: OneZero[18]

In 2022 in Georgia, police arrested Randal Quran Reid while he was driving to his mother's home the day after Thanksgiving for crimes that he was incorrectly accused of committing in Louisiana.[2] He was wrongfully detained in a Georgia jail for six days while awaiting extradition to Louisiana, a state he had never visited. The arrest warrant was based solely on a facial recognition technology match, which the detective failed to disclose in the arrest affidavit.[3]

In Detroit, an eight-month-pregnant mother of two was falsely arrested for carjacking and robbery.[4] She was questioned by police for 11 hours. While in custody, she began to experience contractions. This was the third case of its kind involving the Detroit Police Department, which uses a facial recognition vendor called DataWorks Plus to run an average of 125 facial recognition searches a year, almost entirely on Black men.[5]

While Black people are most frequently harmed by false leads based on facial recognition technology, people of all genders and races are susceptible to misidentification.

In Colorado in 2015, a white man named Steve Talley was charged by Denver prosecutors with bank robbery and assaulting a police officer based on a facial recognition match. The facial recognition technology confirmed a match despite clear physical differences between the suspect and Talley, including a three-inch difference in height and a mole on Mr. Talley's right cheek. Talley successfully fought the charges, but not before he lost his house, his job and custody of his children. He sued the City of Denver and its police department for false arrest, excessive force and malicious prosecution, alleging that their actions ruined his career in finance and left him unhoused and unable to see his children for two years.[6]

When biometric technologies *do* work, the results can be alarming.

Even when biometric data technology works as intended, the results can invite egregious violations of civil rights and civil liberties. Biometric data can track an individual's movements, activities and associations with alarming consistency and lack of oversight.

Targeting Opposition

In New York, the Chief Executive of Madison Square Garden Entertainment Corp. forbids any attorney that has sued Madison Square Garden from entering the venue. To do so, he uses facial recognition technology and photos of the attorneys posted online to identify and turn them away at the door.[7] This example provides a window into a future where anyone — whether a corporation, individual or government — can use these technologies to target people they disagree with.

Government Abuse

The FBI has already collected DNA samples from 21 million Americans, largely via third-party collectors including family ancestry websites.[8] That's more than three times the population of the state of Colorado.[9] Mass collection of biometric data without consent, oversight or regulation can lead to discrimination and enable violations of civil

Figure 1

>6,000,000 people
Approximate population of Colorado

21,000,000 people
Approximate size of FBI DNA sample bank

Source: U.S. Census Bureau and Wall Street Journal

rights and civil liberties.

Private entities fail to protect biometric data.

Case Study One: Amazon

In 2018, the American Civil Liberties Union (ACLU) called for Amazon to stop selling its facial recognition tool to governments for surveillance purposes.[10] While CEO Jeff Bezos acknowledged that Amazon's technologies might be put to "bad uses," he suggested that society's "immune response" would kick in and solve the problem.[11] It took two years of zealous advocacy by civil rights and tech privacy groups for Amazon to issue a one-year moratorium on selling its facial recognition technology to law enforcement.[12] Although the company has since extended that moratorium indefinitely, its internal policy — subject to change at any time — is the only force guiding that decision.[13]

Amazon has since introduced palm-scanning technology that can be found nationwide at stadiums, Whole Foods, Starbucks, Panera and Amazon Go store locations. To access this "palm-based identity service," Amazon needs images of your palm, government-issued ID, payment information and face.[14] Safeguards for biometric data privacy must apply to this additional technology, which is already the subject of litigation against Amazon and Starbucks in Washington and New York.[15] Those lawsuits allege that the companies failed to inform consumers that their biometric information was being collected or get consent for that collection.

Case Study Two: Clearview AI

The company Clearview AI created a facial recognition technology that was allegedly on track to have captured 10 billion faceprints — equivalent to 14 photos for each of the seven billion people on Earth. To create the tool, the company scraped images from Facebook and other websites without obtaining consent.[16] The technology was marketed to hundreds of law enforcement agencies.[17]

The ACLU of Illinois challenged Clearview AI's actions in court under the Illinois Biometric Information Privacy Act. Pursuant to the settlement in 2022, Clearview AI has been permanently banned from selling its faceprint database to most businesses and other private entities across the United States. It was also banned for five years from selling its database to any entity in Illinois, including state and local police.

How is biometric data protected under Colorado law?

In Colorado, there is currently no prohibition on a corporation selling or trading biometric data. Any time someone uses a biometric data technology service — even doing something as banal as trying sunglasses on online — their biometric data could end up in the hands of dozens of other entities that will use it for completely unrelated reasons. This data can be traded again and again, sold from company to company, without the original data owner ever knowing.

Colorado needs biometric privacy legislation.

This legislative session, the ACLU of Colorado is working on a bipartisan bill sponsored by Representative Lindsey Daugherty and Senator Paul Lundeen to better protect biometric data privacy. The bill will amend the Colorado Privacy Act to:

- Require that corporations obtain an individual's consent before collecting and using their biometric data;
- Prohibit biometric data from being sold or traded outside of the company that collected it;
- Require businesses to delete a person's biometric data one year after an individual last interacted with the business or upon the individual's request;
- Give people the right to find out which companies have their biometric data and what specific data they have; and
- Allow law enforcement agencies to continue accessing these types of data through a warrant or subpoena but disallow their bulk purchase of this information from corporations.

Who supports this legislation?

As is the case with many other privacy issues, concerns about biometric data are non-partisan. Progressives, moderates, conservatives and libertarians all support protecting Coloradans' biometric data.

Endnotes

1 Jennifer Henderson, “Black Mom Sues City Of Detroit Claiming She Was Falsely Arrested While 8 Months Pregnant By Officers Using Facial Recognition Technology,” CNN, August 8, 2023, https://www.cnn.com/2023/08/07/ us/detroit-facial-recognition-technology-false-arrestlawsuit/index.html.

2 Sudhin Thanawala, “Facial Recognition Technology Jailed A Man For Days. His Lawsuit Joins Others From Black Plaintiffs,” AP News, September 24, 2023, https://apnews. com/article/mistaken-arrests-facial-recognitiontechnology-lawsuits-b613161c56472459df683f54320d 08a7.

3 Kashmir Hill & Ryan Mac, “Thousands of Dollars for Something I Didn’t Do,” NY Times, March 31, 2023, https:// www.nytimes.com/2023/03/31/technology/facialrecognition-false-arrests.html.

4 Joey Cappelletti, “Pregnant Woman’s Arrest In Carjacking Case Spurs Call To End Detroit Police Facial Recognition,” AP News, August 7, 2023, https://apnews.com/article/detroitpolice-facial-recognition-lawsuit-cab0ae44c1671fc30617 d301b21b2d13.

5 Kashmir Hill, “Eight Months Pregnant and Arrested After False Facial Recognition Match,” NY Times, August 6, 2023, https://www.nytimes.com/2023/08/06/business/facialrecognition-false-arrest.html.

6 See Rob Low, “Man Arrested Twice For Bank Robbery Sues Denver, Police And FBI For $10 Million, Fox 31 Denver,” September 15, 2016, https://kdvr.com/news/man-arrested-twice-for-bank-robbery-sues-denver-police-and-fbi-for-10-million/; Alan Prendergast, Steven Talley, Wrongly Accused of Bank Robberies, Featured on Dark Net (May 3, 2017) https://www.westword.com/news/steven-talley-featured-on-showtimes-dark-net-9026953.

7 Kashmir Hill & Corey Kilgannon, “Madison Square Garden Uses Facial Recognition to Ban Its Owner’s Enemies,” NY Times, January 3, 2023, https://www.nytimes. com/2022/12/22/nyregion/madison-square-gardenfacial-recognition.html.

8 Ken Klippenstein, “FBI Hoovering Up DNA At A Pace That Rivals China, Holds 21 Million Samples and Counting,” The Intercept, August 29, 2023, https://theintercept.com/2023/08/29/fbi-dna-collection-surveillance/; Amy Dockser Marcus, “Customers Handed Over Their DNA. The Company Let the FBI Take a Look,” WSJ, August 22, 2019, https://www.wsj.com/articles/customers-handed-over-their-dna-the-company-let-thefbi-take-a-look-11566491162.

9 “The United States Census Bureau estimates the population of Colorado to be 5,877,610 people as of July 1, 2023,” QuickFacts Colorado, U.S. Census Bureau, accessed January 8, 2024, https:// www.census.gov/quickfacts/fact/table/CO.

10 Matt Cagle & Nicole Ozer, “Amazon Teams Up With Government to Deploy Dangerous New Facial Recognition Technology,” ACLU, May 22, 2018, https://www.aclu.org/news/privacy-technology/amazon-teams-government-deploy-dangerous-new.

11 Nicole Ozer, “Face Recognition Tech Presents A Surveillance Issue And Amazon Is Running Amok,” USA Today, January 20, 2019, https://www.usatoday.com/story/ opinion/2019/01/20/face-recognition-surveillance-issueamazon-google-microsoft-column/2581992002/.

12 Karen Hao, “The Two-Year Fight To Stop Amazon From Selling Face Recognition To The Police,” MIT Technology Review, June 12, 2020, https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/.

13 Karen Weise, “Amazon Indefinitely Extends A Moratorium On The Police Use Of Its Facial Recognition Software,” NY Times, May 18, 2021, https://www.nytimes. com/2021/05/18/business/amazon-police-facialrecognition.html.

14 Emma Roth, “Amazon’s Palm-Scanning Technology Can Let You Buy A Drink Without Getting Out Your ID,” The Verge, May 22, 2023. https://www.theverge.com/2023/5/22/23732823/amazon-one-palm-scanning-technology-age-verification.

15 See Lauren Rosenblatt, “Amazon, Starbucks Face WA Class-Action Lawsuit Over Customer Data,” Seattle Times, June 8, 2023, https://www.seattletimes.com/business/ amazon-starbucks-face-wa-class-action-lawsuit-overcustomer-data/; Leif Weatherby, “Amazon’s ‘Just Walk Out’ Tech Is a Privacy Nightmare,” Daily Beast, August 14, 2023, https://www.thedailybeast.com/amazons-just-walk-outfrictionless-checkout-tech-is-a-privacy-nightmare.

16 In Big Win, “Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law,” ACLU, May 9, 2022, https://www.aclu.org/press-releases/ big-win-settlement-ensures-clearview-ai-complies-withgroundbreaking-illinois.

17 Kashmir Hill, “The Secretive Company That Might End Privacy as We Know It,” NY Times, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html?login=email&auth=login-email.

18 See also Dave Gershgorn, “21 states are now vetting unemployment claims with a ‘risky’ facial recognition system, onezero,” February 3 2021, “even the best-performing facial recognition systems . . . do not perform as well on women and people with darker skin tones.”; “in some cases, people with darker skin tones were misidentified at rates 10 to 100 times more often than people with lighter skin tones.”

ACLU
Colorado

303 E. 17th Ave., Suite 350
Denver, CO 80203-1256
aclu-co.org