The Ethics of Biometrics: Navigating the Technological Landscape

Rob Jones
COMP 488
Loyola University Chicago
Fall 2023

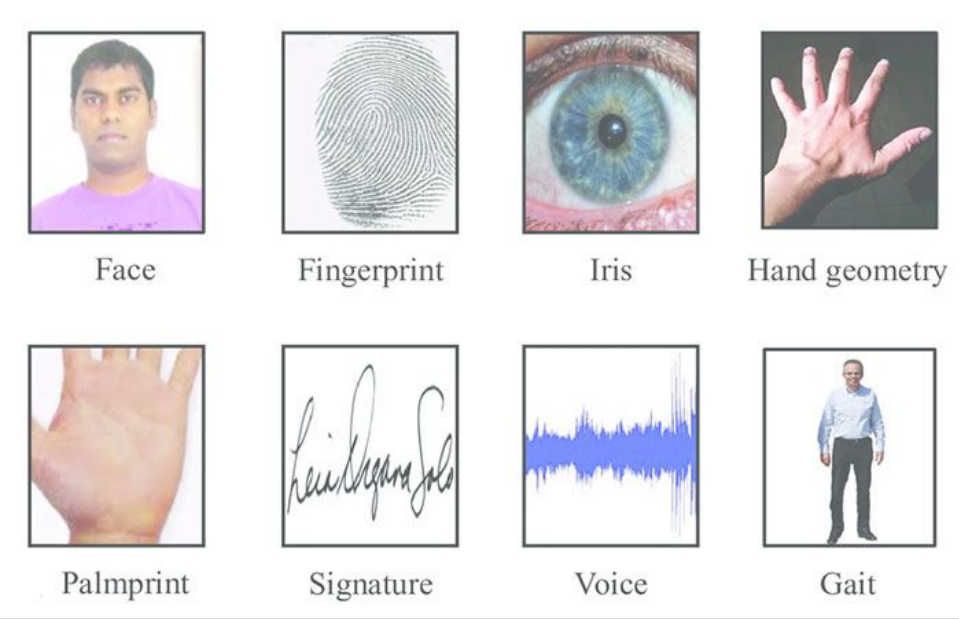
Introduction

- **Overview of Biometrics:**
  - Biometrics involves identifying and authenticating individuals based on unique biological characteristics, offering a reliable and fast method for verification.
  - It encompasses both physiological measurements (e.g. fingerprints, iris patterns) and behavioral measurements (e.g. voice recognition, gait analysis).
- **Significance of Biometrics:**
  - Biometric technology has become increasingly significant due to its widespread applications in various sectors, including law enforcement, healthcare, and commercial industries.
  - Its benefits include higher security and accuracy, providing an alternative to traditional methods like passwords and documents.
- **Objective of the Presentation:**
  - Explore the ethical implications of biometric technology, focusing on privacy concerns, data security, consent, and bias.
  - Discuss how these technologies impact individuals and society, balancing technological advancement with ethical considerations.

What are Biometrics?

- **Definition:**
  - Biometrics are measurements and calculations related to human characteristics, used for identification and access control.

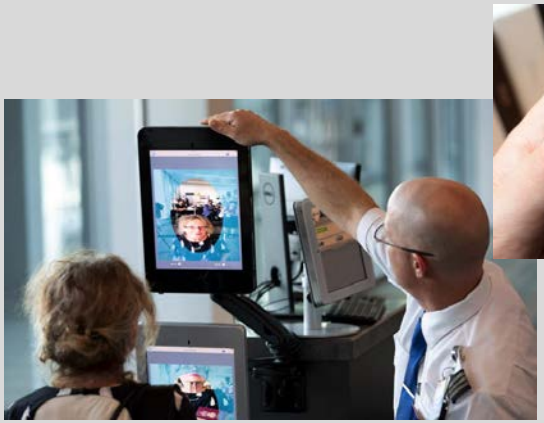
- **Types of Biometric Identifiers:**
  - **Physiological Characteristics:** These are related to the shape of the body and include fingerprints, palm veins, face recognition, DNA, hand geometry, iris recognition, retina patterns, and more.
  - **Behavioral Characteristics:** These involve patterns of behavior and include voice recognition, gait analysis, typing rhythm, and signature dynamics.

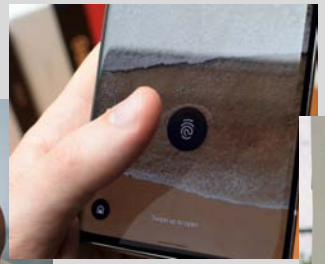


https://www.bayometric.com/biometric-system-architecture/

Applications of Biometrics

- **Overview:**
  - Biometric technologies are increasingly employed across various industries to secure digital transactions and enhance user experiences.
- **Key Sectors Utilizing Biometrics:**
  - **Banking and Financial Services:** Biometrics aid in meeting Know Your Customer regulations, authenticating online customers, and even replacing card swipes at ATMs with facial recognition.
  - **Healthcare:** Used for patient identification, integration with electronic medical records, and telehealth services. Tools include facial, iris recognition, fingerprint scanning, and voice recognition.
  - **Hospitality and Travel:** Essential for airline passenger authentication, biometrics are also used for efficient check-ins at hotels and airports, with facial recognition enabling quick access to services like car rentals.
  - **Payment Processing:** Growing use in transaction security, with companies like Mastercard enabling biometrically transacted payments. Biometrics also provide alternatives to traditional password and PIN security methods
- **Market Growth:**
  - The global biometrics market, valued at $39.62 billion in 2021, is projected to grow significantly, driven by increasing adoption in sectors like military, automotive, and consumer electronics.





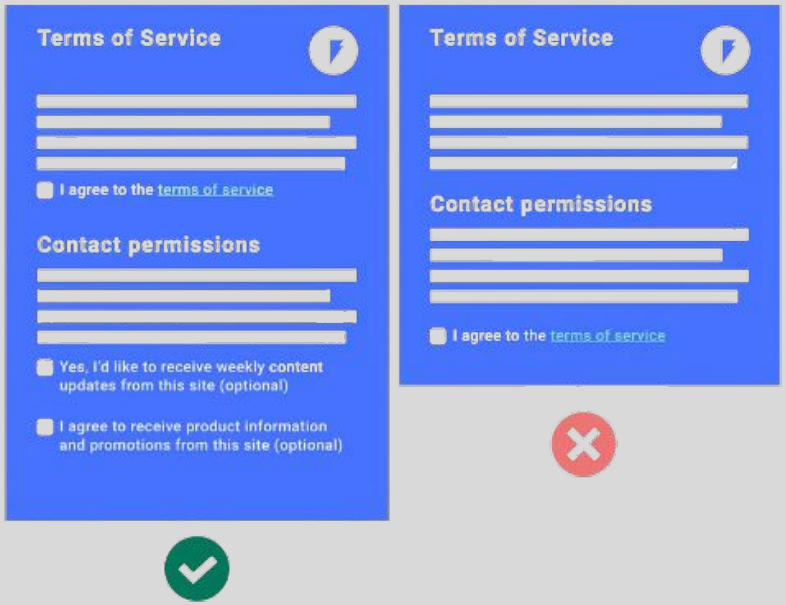
Privacy Concerns

- **Introduction to Privacy Issues:**
  - The expanding use of biometrics raises significant privacy concerns. These technologies are becoming more integrated into daily life, and are a regular part of interactions with governments and private companies.
- **Challenges to Privacy:**
  - **Function Creep:** The risk of biometric data being used for purposes other than originally intended, such as an employer using facial recognition data to monitor employees' attendance.
  - **Covert Collection:** The possibility of collecting biometric data without individuals' knowledge or consent, like capturing facial images or lifting fingerprints without awareness.
  - **Secondary Information Disclosure:** Potential for biometric data to reveal more personal information than intended, such as health conditions from a facial biometric image.
  - **Consent Issues:** Difficulty in obtaining meaningful consent for biometric data collection, especially when it is passive or mandatory, such as in workplaces.
- **Data Security Concerns:**
  - Biometric data security is crucial as it's immutable unlike passwords. Leaked biometric data like fingerprints or retinal scans pose permanent risks to individuals.
  - Risks include data leaks from devices, servers, or software, and the potential for false positives and negatives in recognition systems, which impact reliability and security.
- **Broader Privacy Implications:**
  - Surveillance and monitoring using biometrics might infringe on territorial privacy. DNA collection, for instance, can affect bodily privacy and potentially expose sensitive personal information.
  - The collection and use of biometric data by companies can lead to potential abuses by governments or criminal entities, posing risks to individual freedoms and personal safety.

Data Security

- **Immutable Data:**
  - Biometric identification systems record immutable personal characteristics, which are permanent and unchangeable once compromised or stolen. This immutability poses a risk as it can lead to irreversible damages like identity theft or misuse of personal information.
- **Cost and Complexity:**
  - Implementing biometrics on a large scale is expensive and complex, requiring substantial investment in hardware, software, interoperability, and cloud services. The cost factor also encompasses user training and security resources.
- **Security Tradeoffs:**
  - While biometric systems offer security advantages, they also introduce additional security risks. Issues like data breaches, server penetrations, and spoofing techniques can compromise biometric data, which is highly sought after in illicit markets like the dark web.
- **Accuracy and Reliability:**
  - Biometric systems can suffer from inaccuracy, bias, and false positives, leading to wrongful denials or unauthorized access. Factors like training data bias, machine errors, and compromised biometrics (like a cut finger) affect the reliability of these systems.
- **Interface Challenges:**
  - Biometric interfaces are extending beyond digital screens to our physical bodies, leading to new technical, legal, and ethical concerns. The diverse applications, from active touch-required systems to passive recognition technologies, introduce complex security considerations.
- **Risk of Misuse and Surveillance:**
  - Biometric data, if misused, can serve purposes beyond access control, such as data brokerage, commercial gains, and surveillance. This raises societal concerns about privacy, identity, and human rights. The lack of standards and policies further amplifies these risks.

Consent and Public Awareness

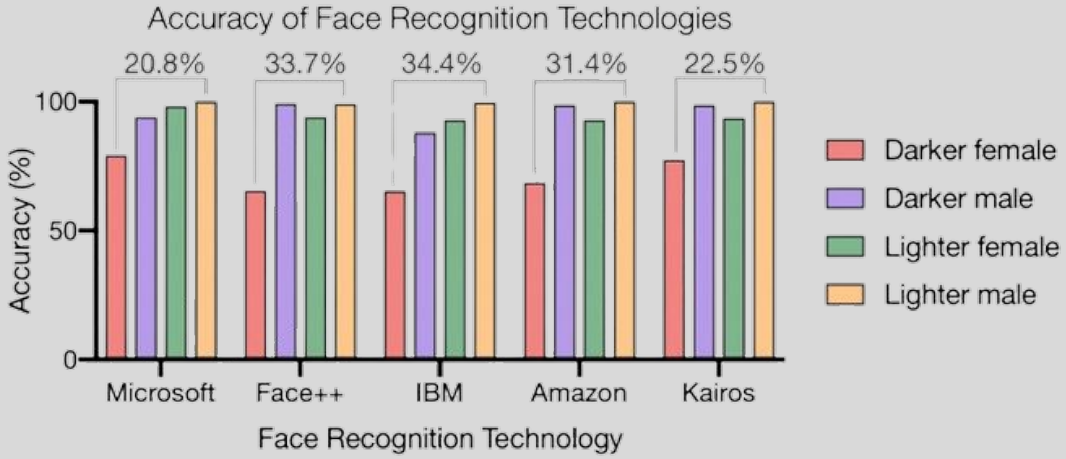


- **Informed Consent in Biometrics:**
  - **Definition:** Informed consent involves clearly informing individuals about how their biometric data will be collected, used, and stored.
  - **Importance:** Ensures ethical data collection practices and respects individuals' privacy and autonomy.
- **Case Study: “Physicals for All” Program:**
  - **Location:** Xinjiang region.
  - **Issue:** Biometric data collected without informed consent, leading to potential human rights violations.
  - **Impact:** Highlights the necessity of transparency in biometric data collection.
- **Raising Public Awareness:**
  - **Objective:** Educate the public on their rights and the implications of biometric data collection.
  - **Methods:** Use of media campaigns, educational programs, and public forums.
- **Collaborative Efforts for Ethical Practices:**
  - **Partnership:** Biometrics Institute and the UN Migration Agency.
  - **Goal:** Promote responsible and ethical use of biometric technology.

Bias and Discrimination

- **Examples of Bias:**
  - Facial Recognition Technology:
    - Significant racial bias, especially against Black people
    - Poorer accuracy in identifying female, Black, and 18-30 year old subjects, with error rates up to 34% higher for darker-skinned females compared to lighter-skinned males.
  - Misidentification Issues:
    - IBM, Microsoft, and Amazon have acknowledged and attempted to reduce bias in their technologies. However, Amazon's Rekognition showed a 31% error in gender classification for darker-skinned women.
  - Application in Law Enforcement:
    - Concerns about face recognition technologies being used disproportionately against marginalized communities, including Black Americans, undocumented immigrants, and Muslim citizens.
    - Racially biased policing strategies lead to overrepresentation of Black people in surveillance systems, creating a feed-forward loop of disproportionate arrests and surveillance.

- **Impact of Bias:**
  - Privacy and Civil Rights:
    - Surveillance threatens rights including privacy, freedom of expression, and due process. It can lead to self-censorship and avoidance of activism.
  - Misidentification and Legal Ramifications:
    - Biased technologies can misidentify individuals, leading to wrongful arrests and incarceration.



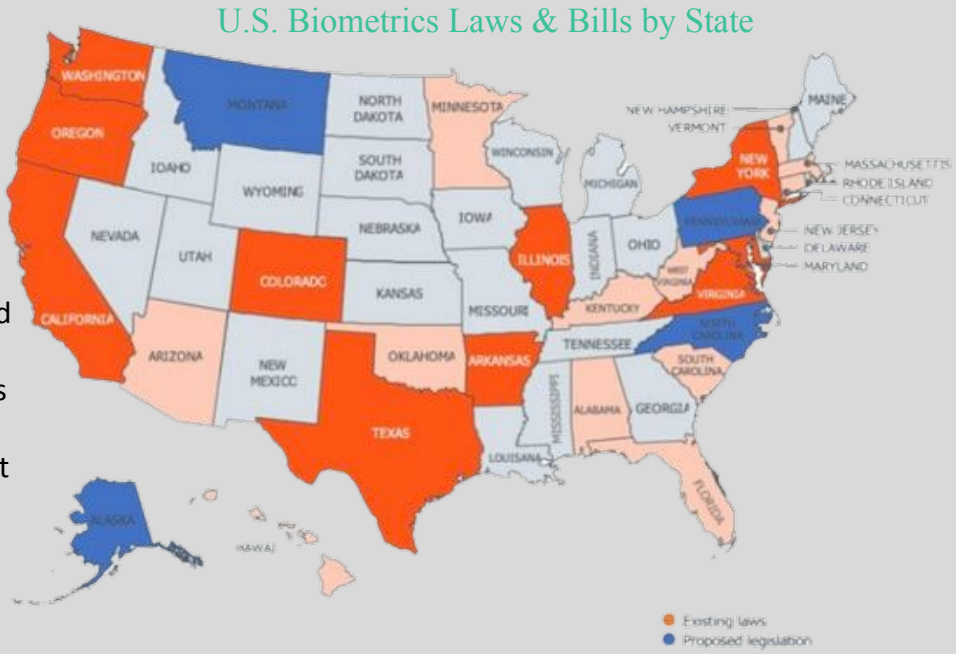
https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/#:~:text=,skinned%20males

Regulatory Landscape

- **Illinois' Biometric Information Privacy Act (BIPA)**
  - Passed in 2008, Illinois was the first U.S. state to adopt biometric legislation. Since then many other states have either passed or proposed similar legislation.
  - BIPA calls for companies and organizations who collect biometric data to gain the consent of individuals in the collection of their biometric data, destroy biometric identifiers in a timely manner, and follow practices for the secure storage of biometric data .

- **European Union General Data Protection Regulation (GDPR)**
  - Passed in 2018, GDPR regulates information privacy and classified biometric data as sensitive data. This classification requires informed consent with provisions for storage and security.
  - GDPR allows for the collection of biometric data. Except in certain circumstances, the collected data cannot be used to uniquely identify an individual.

- **Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act**
  - In 2023 the FTC issued a commitment to combating "unfair or deceptive acts and practices related to the collection and use of consumers' biometric information and the marketing and use of biometric information technologies".



https://www.mondaq.com/unitedstates/privacy-protection/1068486/us-biometric-laws--pending-legislation-tracker

Case Study - Positive Use

- **Beneficial uses of biometrics:**
  - **Accuracy and security**: Increased accuracy in personal identification and authentication increases the reliability of security procedures.
  - **Ease of use**: Since biometric markers are a part of a person, there is no need to remember passwords or carry security devices such as ID cards or fobs.
  - **Time saving**: Similar to the above, biometric markers are immutable meaning there is no need for password resets or other traditional time consuming security measures.
  - **Fraud reduction**: Biometrics as identity verification cannot be forged, brute forced, or easily guessed decreasing the risk of hacking or fraudulent behavior.

- **Case Study:** 2018 UN verification of refugees in Uganda
  - **Issue:** With over 1.4 million refugees in camps, the process for administering aid and providing food at these locations was fraught with fraud and mismanagement.
  - **Solution:** Representatives collected the biometric data of 1.1 million refugees. This data was used for verification when handing out food and assistance leading to a reduction in fraud, waste, and an overall improvement in the management of the camps.

- **Case Study:** Biometric smart payment cards
  - **Issue:** Many people struggle with point-of-sale systems at retail locations due to things such as an inability to see the numbers on the keypad or remember their PIN number.
  - **Solution:** Payment and banking cards with finger scanners allow transactions to be completed only while in the hand of the owner. This makes payment cards more secure, user-friendly, and limits the need for immunocompromised people to interact with pin pads.

Case Study - Ethical Concerns

- **Case Study:** 2015 & 2020 Facial recognition for identifying protestors
  - **Location:** Baltimore, Maryland and at least 15 other U.S. cities
  - After the death of Freddie Gray in 2015 the Baltimore Police Department used facial recognition to identify protestors. Similarly, after the death of George Floyd in 2020 the Department of Homeland Security used drones and helicopters for facial recognition during protests. This use of facial recognition can be seen as an issue of civil liberties.

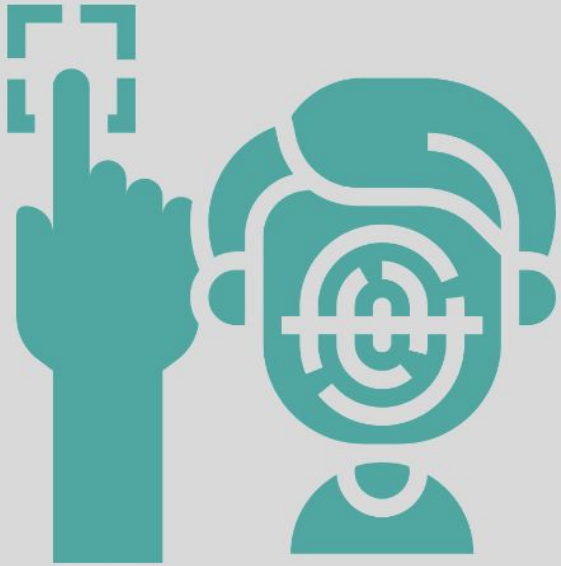
- **Case Study:** 2019 & 2020 Wrongful convictions of Nijeer Parks, Robert Williams, and Michael Oliver
  - **Location:** Detroit, Michigan; Woodbridge, N.J.
  - All three men were wrongfully arrested and accused of crimes they did not commit due to misidentification by the police department's facial recognition technology.

- **Case Study:** 2022 Madison Square Garden Entertainment bans lawyers
  - **Location:** New York, New York
  - Upon entry to venues owned by MSG Entertainment ticket holders identified by facial recognition system on an "attorney exclusion list" are asked to leave immediately without gaining access to the event. This list is comprised of any attorney that work for a law firm in litigation with MSG Entertainment. It was created by scraping the publicly available profile photos and information from the law firms' websites.

- **Case Study:** An example of biometric data in the wrong hands - Handheld Interagency Identity Detection Equipment (HIIDES) system
  - **Location:** Iraq & Afghanistan
  - The U.S. military created a biometric data system for the identification and classification of individuals. For ease of use in the field, the system was neither classified nor encrypted creating an open database of personal information. This system was later used by the Taliban for targeting individuals who had been U.S. allies.

Conclusion

- Biometric technologies have significantly advanced, integrating into various sectors for identification and security purposes.
- Key ethical concerns include privacy, data security, and potential biases in technology. It's essential to maintain a balance between innovation and ethical responsibility, ensuring the fair and secure use of biometrics.



Questions?

Sources

"Biometrics and Privacy - Issues and Challenges." *Office of the Victorian Information Commissioner*, 6 Oct. 2022, ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/.

Burt, Chris. "Biometrics Institute Discusses Importance of Informed Consent and Purpose: Biometric Update." *Biometric Update | Biometrics News, Companies and Explainers*, BiometricUpdate.com, 23 Jan. 2018, www.biometricupdate.com/201801/biometrics-institute-discusses-importance-of-informed-consent-and-purpose.

Daniel.farrell. "7 Key Benefits of Security with Biometrics." *GlobalSign*, 7 Feb. 2020, www.globalsign.com/en/blog/7-benefits-security-with-biometrics.

"The Ethical Implications and Legal Responsibilities of Biometric Data Security." *Best Identity Access Management (IAM) Software, Tools, Vendors, Solutions, & Services*, 24 Aug. 2022, solutionsreview.com/identity-management/the-ethical-implications-and-legal-responsibilities-of-biometric-data-security/#:~:text=However%2C%20like%20all%20data%2C%20biometrics,ethical%20implications%2C%20risks%2C%20and%20benefits.

Ethical Principles for Biometrics - Biometrics Institute, www.biometricsinstitute.org/wp-content/uploads/Biometrics-Institute-Ethical-Principles-Final_1019-1.pdf. Accessed 4 Dec. 2023.

"Ethics in Biometrics: What Every Security Management Professional Should Know." *ASIS Homepage*, www.asisonline.org/publications--resources/news/blog/ethics-in-biometrics-what-every-security-management--professional-should-know/#:~:text=In%20response%20to%20the%20burgeoning,%E2%80%9CEthical%20Use%20of%20Biometric%20Technology%E2%80%9D.

Eugenie Park, Darrell M. West, and Trisha Ray Pranay Kotasthane. "The Enduring Risks Posed by Biometric Identification Systems." *Brookings*, 9 Feb. 2022, www.brookings.edu/articles/the-enduring-risks-posed-by-biometric-identification-systems/.

Sources Continued

Hill, Kashmir, and Corey Kilgannon. “Madison Square Garden Uses Facial Recognition to Ban Its Owner’s Enemies.” *The New York Times*, The New York Times, 22 Dec. 2022, www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html.

Kerry, Cameron F., et al. “Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color.” *Brookings*, 27 Sept. 2023, www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

Marketing, Blueflamingo. “How Biometric Technology Can Support Vulnerable Members of Society?” *IDEX Biometrics*, 23 Dec. 2020, www.idexbiometrics.com/how-biometric-technology-can-support-vulnerable-members-of-society/.

Morais, Lenildo. “Biometric Data: Increased Security and Risks.” *Security Magazine RSS*, Security Magazine, 5 May 2020, www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks.

“OPM and UNHCR Complete Countrywide Biometric Refugee Verification Exercise - Uganda.” *ReliefWeb*, 29 Oct. 2018, reliefweb.int/report/uganda/opm-and-unhcr-complete-countrywide-biometric-refugee-verification-exercise.

Ritchie, John Newman & Amy, and Nick Jones. “FTC Warns about Misuses of Biometric Information and Harm to Consumers.” *Federal Trade Commission*, 18 May 2023, www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.

SITNFlash. “Racial Discrimination in Face Recognition Technology.” *Science in the News*, 26 Oct. 2020, sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/#:~:text=,skinned%20males.