Facial Recognition Software

Dan Salerno, Jenn Cafiero, Max Remetz

Summary of Article

- Facial recognition is a form of biometric artificial intelligence that can uniquely identify a person by analyzing patterns in the person’s facial texture and shape
- There are still very few federal regulations for how it is used
- The capabilities of facial recognition for surveillance purposes has led for some groups to call for a ban on police use

Technology Involved

- Facial recognition software
- Surveillance hardware and software including security cameras and smartphone devices
- Federal or statewide identification databases (i.e. DMV database)

Stakeholders

- General Population
- Law enforcement
- Government
- Technology Companies

Major Impacts

- General Population
  - Decrease in privacy
  - New data security concerns
- Police
  - New tool for police work
    - Where does this tool exist?
    - Balancing bias
  - Possible public scrutiny for using the tool

Major Impacts

- Government
  - Need to come up with regulations on facial recognition
    - Should it even be regulated/how much should it be regulated?
- Tech companies
  - New space to expand into ($)
  - Their role in regulation

Advantages

- General Population
  - Possible increase in safety and peace of mind
  - Could pave the way for more uses of facial recognition
- Police
  - More effective policing
  - Could save money and time for the police force

Advantages

- Government
  - Help keep society safer and prevent crime
  - Could use data gathered from facial recognition for other uses
- Tech companies
  - Make money
  - Contribute to the benefit of society

Disadvantages

- General Population
  - Privacy and consent concerns
  - As more places adopt these systems, it could be hard to find somewhere to live “off grid”
- Police
  - Possible abuse of the system
  - Cost and growing pains that come with the use of a new tool

Disadvantages

- Government
  - Hard to ensure that the proposed regulation is effective
    - Checks and balances
  - Could shift toward more authoritarian governing style
- Tech companies
  - Hard to ensure that the system is unbiased
  - Could be risky to develop these systems if government or social opinions change

Other Issues/Challenges

- Nobody is entirely sure that an unbiased facial recognition system can be created
  - Many facial recognition algorithms still show higher error rates for African-Americans, women, and young people
  - Available training data sets may have biases that can't be corrected, which makes the system have bias by default
    - E.g. using mugshots can be biased because of how police enforcement includes racial bias over the years

Ethical Concerns

- Invasion of Privacy
  - Government/Business tracking of individuals based on recognition
  - Collection and storage of facial recognition data (i.e. your face)
  - Face-recognition app sparks controversy after it's reportedly used to track women who appeared in porn films

- Potential bias
  - higher error rates across different demographics
  - bias in data used for training

Code of Ethics Standards

1. **Public** - Software engineers shall act consistently with public interest
2. **Client and Employer** - Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest
3. **Product** - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible
4. **Judgement** - Software engineers shall maintain integrity and independence in their professional judgment
5. **Management** - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.

Code of Ethics

Public/Client Interest

- Privacy violations v.s. Effective Security

Product, Judgement

- Reduce bias and error in software

Management

- Adhere to ethical standards/regulations for vision of product

Stances

1. **Pro regulation** on facial recognition technology
2. **No regulation** on facial recognition technology
3. **Complete ban** on the use of facial recognition

Stance 1: Pro Regulation on Technology

“There is a need for regulation in this space, both for law enforcement and even private companies in certain use cases… Particularly in private sector use, there is a relationship between our customer and the individual, so they should be able to get consent.”

- Brian Brackeen, CEO of the facial recognition company Kairos

Stance 2: No regulation on Technology

“People forget the benefits. That gets drowned out. This is a wildly successful technology that’s been used to stop terrorist attacks. It’s been used to take criminals off the street...It makes people’s lives better. And I think those benefits get lost in all the negativity.”

- *Benji Hutchinson, VP of federal operations at NEC America*

Stance 3: Complete Ban on Technology

“What does it take to get the public on board with a massive facial recognition infrastructure? Don’t just make them comfortable with facial recognition technology, engineer the desire for it. This is what the consumer side of facial recognition technology is doing: making it seem banal and unworthy of concern.”

- *Evan Selinger, philosophy professor at Rochester Institute of Technology*

Possible Solutions

Strong regulation on use of facial recognition software/data

- Consent requirements
- Performance Standards

Ban/Limit usage in certain fields

- Police usage (i.e. warrants, phone-tapping parallel?)
- Commercial Usage