Who Goes There?

Issues in Facial Recognition + Surveillance

Ayushi Sinha '20 (ayushis)

Agenda

What is Facial Recognition?

A system that can identify an individual from an image or video

How does it work?

Capture your face from a still image or video

Your face is compared to a database of known faces + a determination is made, often presented with a confidence score

Step #1

Step #2

Step #3

Facial Recognition Software reads your face geometry + identifies facial landmarks (e.g. distance between eyes to create a **facial signature.**)

https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

How does it work?

Capture your face from a still image or video

Your face is compared to a database of known faces + a determination is made, often presented with a confidence score

Step #1

Step #2

Step #3

Facial Recognition Software reads your face geometry + identifies facial landmarks (e.g. distance between eyes to create a **facial signature.**

How does it work?

Capture your face from a still image or video

Your face is compared to a database of known faces + a determination is made, often presented with a confidence score

Step #1

Step #2

Step #3

Facial Recognition Software reads your face geometry + identifies facial landmarks (e.g. distance between eyes to create a **facial signature.**

https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

Features of Facial Recognition: Microsoft Azure Face

Face Identification

"Face API enables you to search, identify, and match faces in your private repository of up to 1 million people."

Similar face search

"Easily find similar-looking faces. Given a collection of faces and a new face as a query, this API will return a collection of similar faces."

Face Grouping

"Organize many unidentified faces together into groups, based on their visual similarity."

Face Verfication

"Check the likelihood that two faces belong to the same person. The API will return a confidence score about how likely it is that the two faces belong to one person."

Features of Facial Recognition: Paravision

- **Face Detection 1:N**

  Identify the existence and location of faces within a photo or set of photos. Gaze detection   within a face or set of faces

- **Face Verification 1:1**

  1:1 face comparison. Used in digital and physical authorization scenarios

- **Face Identification**

  1 to many face search. Used for identifying "faces in a crowd" and clustering across thousands   of hours of video

- **Face Clustering**

  Used to cluster togethers groups of similar faces or faces that share certain attributes

- **Spoof Detection**

  Combat paper, screen, mask and virtual avatar based presentation attacks

- **Age Estimation**

  Using facial landmarks and occlusions, estimate the age of a face

- **Gender Detection**

  Estimate whether a face belongs to a male or female

- **Phenotype Detection**

  Determine the ethnicity or phenotype of a person based on their facial attributes

- **Emotion Detection**

  Determine what people are doing in a scene

- **Real-time Streaming**

  Detect, identify and verify faces in live streaming video for immediate alerts and data."
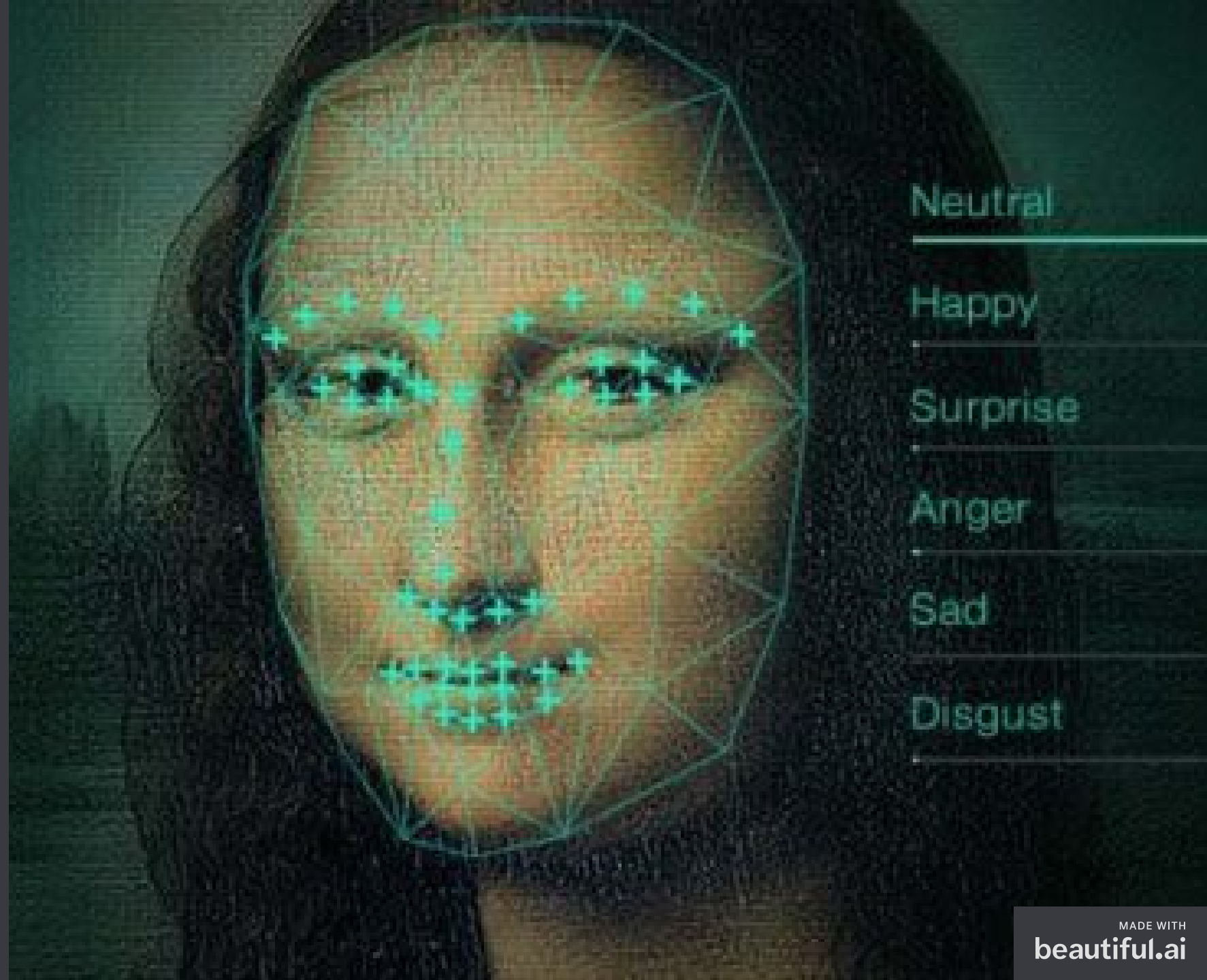
Applications

Surveillance

Identification

Retail

Hiring

MADE WITH
beautiful.ai

Case Studies

Neutral

Happy

Surprise

Anger

Sad

Disgust

China

Facial Recognition is being used to catch jaywalkers, surveil Uyghurs (Muslim minority group), and identify protestors in Hong Kong.

U.S. Surveillance

Police Body Cams, IoT Devices

Recruiting

Hirevue claims to expand opportunity, but without insight into the explainability of the system

- AI Blackbox Legal Protection

- Explainability

  Do we need evaluation criteria and explainability of the system prior to using? Does accuracy of the system affect our answer?

Commercial

Coffee Shops, Retail, and More...

Thorn

Applying Facial Recognition to Combat Human Trafficking

- Do we have enough information and data on those trafficked for the use of this technology to be feasible?

- How can we balance using facial recognition for good with other, potentially unethical, practices?

- What should our views be towards sharing visual data?

Regulation

There's no federal regulation. This is one level of proposing regulation. At what level should regulation be imposed? Is this effective?

1 **Enrollment**

Where do we get initial data? This needs to be more strongly regulated

2 **Real time footage aquisition**

Where are we placing cameras? How does Ring/Nest fit in?

3 **Biometric matching**

We need to safeguard the database + matchmaking process. Prevent this from ever being on a public domain

4 **Applications of the identification**

Search warrant + due process of law driver's license fraud)

Discussion Questions

- How to balance collective security with individual privacy?

  Where do commercial interests fall into this?

- How does facial recognition change the nature of identification and protest?

- What are the moral, ethical, legal implications of applying this technology?

  How does this change based on the case study? Should we note other factors that affect permissibility?

- Should we regulate facial recognition?

  If so, how and to what extent?

  Should we take the public and private applications into account?

- Who should have a say in regulation?

  How is this complicated when one branch of the government (legislative) must audit another (executive)? This is multinational, how do we regulate this? Sanctuary cities? What's our responsibility as creators of this technology?

Solution?

Can we design a platform to license facial data? How can we incentivize both sides of this market? Synthetic Data?