Beyond

FACEVALUE

Smile! :)
You're on
the camera.

Truth is coming, and it cannot be stopped.

- Edward Snowden, Former CIA employee

Contents

Holborn Station, London

Moving towards a surveillance state in UK with the rise of facial recognition and its disguised use becoming a norm. Are the new EU GDPR guidelines unintentionally creating a path of camouflaged spying? Is the crime rate decreasing or is it just the privacy being harmed?

Research Question.

UK Police body camera - https://www.bbc.co.uk/news/

Technology is expanding and evolving, even as I am writing this report for submission. Society, including the law enforcement is struggling to keep up the pace with all the daily developments in technology. To keep up with the pace of the technology the surveillance is increasing in the form of Closed-circuit television (CCTV) cameras. According to Wong Dennis's (2019) report Big brother is watching you: the world's top 100 most surveilled cities the cameras in china have gone from 40 million in 2014 to 200 million in 2018.

This doesn't come as a shock to me, but the matter for fact that London is the 6th most surveilled city in the world, is something which is really shocking! As the Wong Dennis mentions in his report.

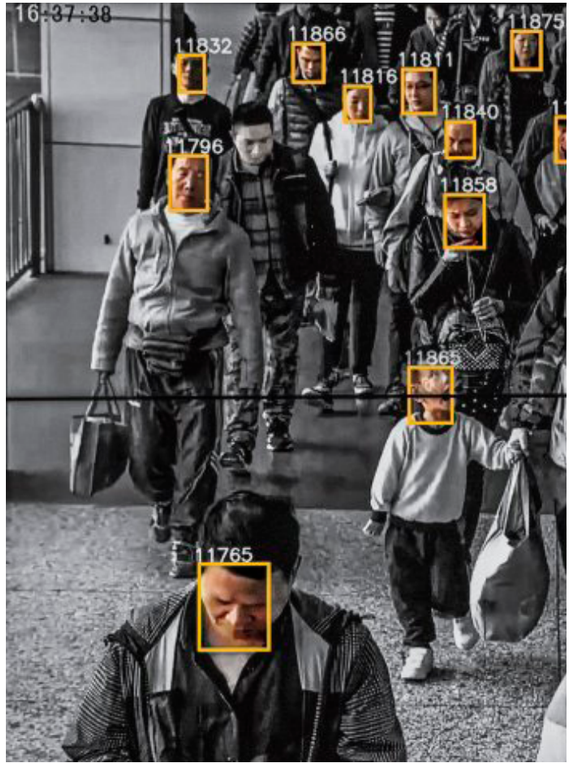
Introduction

Art Background - Cameras: Shantou University

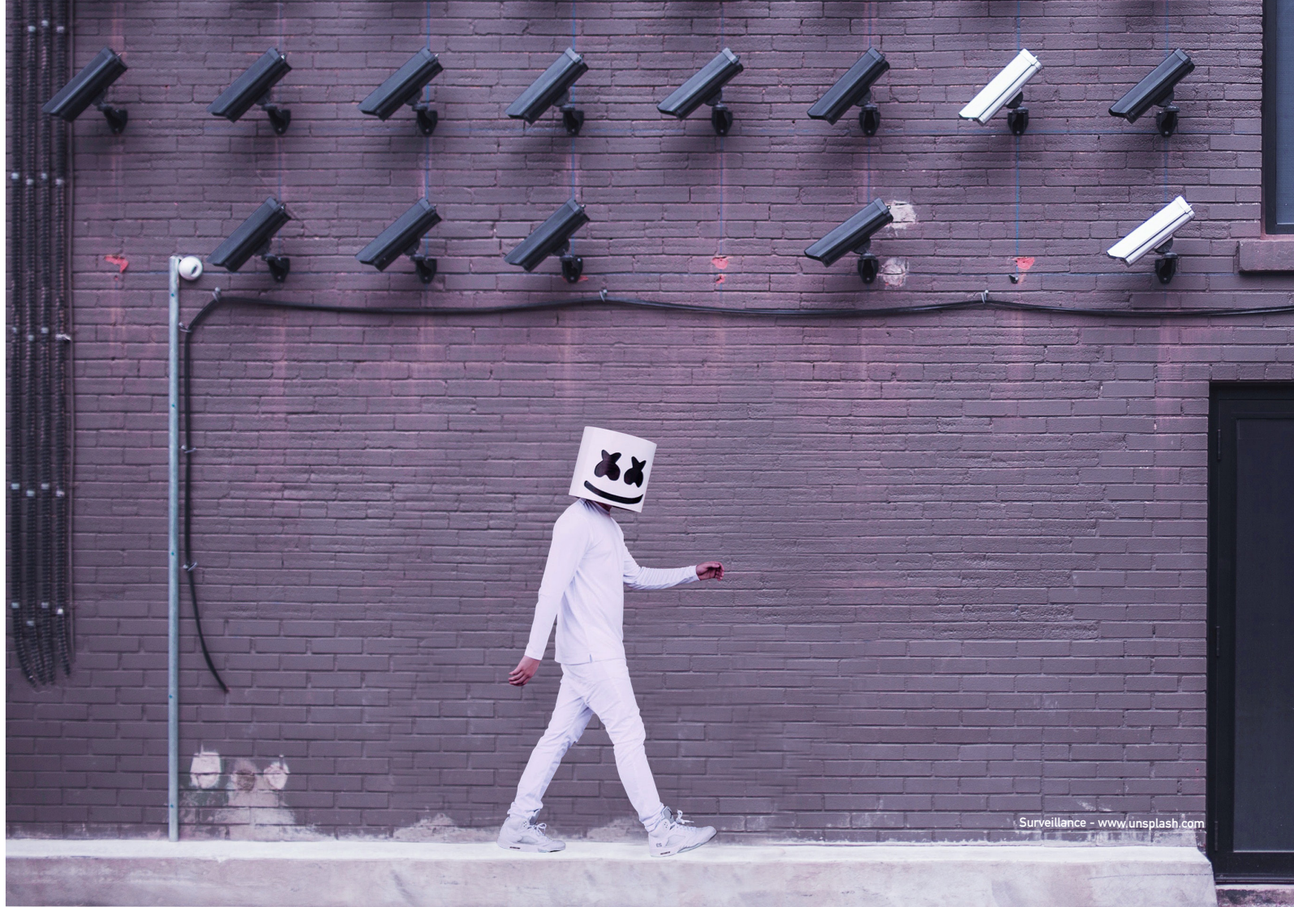
The research of this project takes a lot of different turns exploring a variety of things related to Facial Recognition Tech, including how it can be avoided and by passed on daily basis. Experimented with a variety of existing approaches like CVdazzle and with multiple algorithms (OpenCV and FaceOsc).

Also briefly discuss the General Data Protection Regulation (GDPR) laws regarding the surveillance using Facial Recognition technology in United Kingdom.

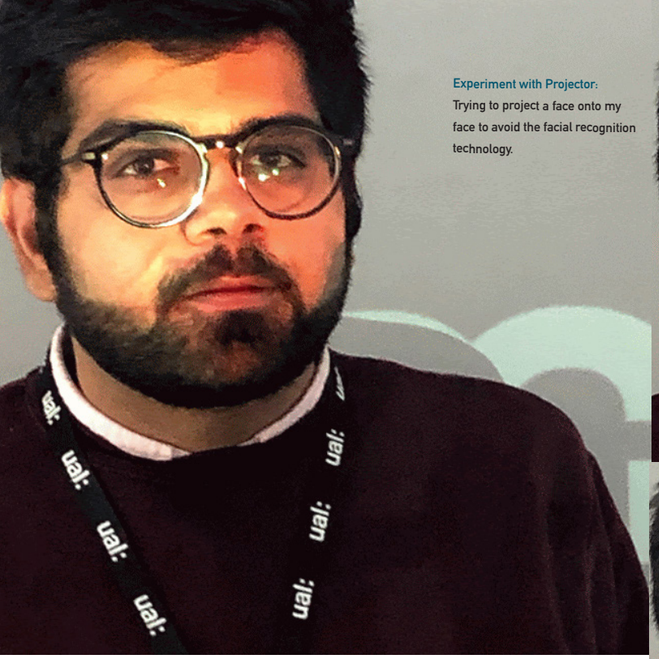
The numbers are speaking of itself that, the surveillance has increased over the years, as mentioned by Wong Dennis (2019) Big brother is watching you: the world's top 100 most surveilled cities. Is the surveillance a breach of privacy? Is it actually keeping "us" safe? The analysis of this project tries to provide the answer to these questions.



China Surveillance - www.wired.co.uk



Surveillance - www.unsplash.com



Experiment with Projector:
Trying to project a face onto my face to avoid the facial recognition technology.

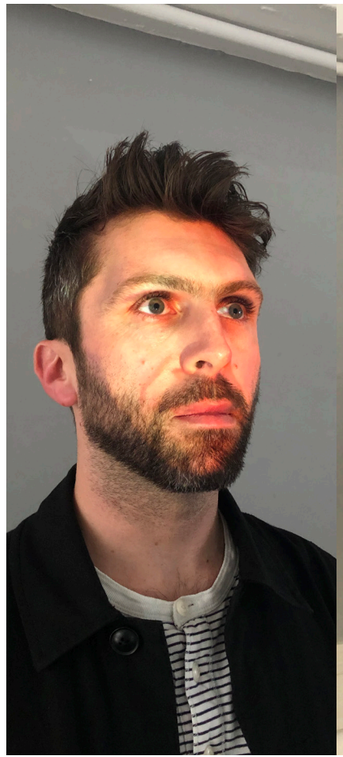
Aim.
Motivation.

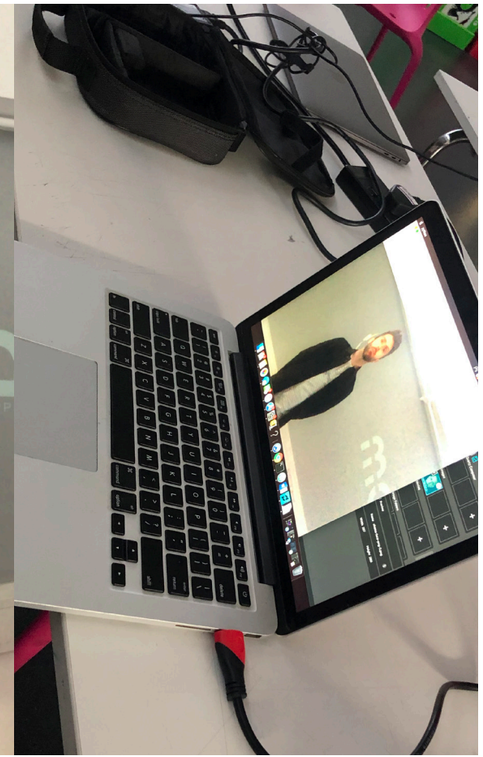
Working with Different angles.

Outcome of the project is to seek awareness from the audience on, "How Surveilled is your city?"

An interactive map which explores various different countries and their level of facial recognition surveillance including the number of CCTV cameras, number of CCTV cameras per 1000 people. Analysing it with the security and crime index of the city and country.

Experimenting with different faces, people, lighting, angles and objects. Avoiding facial recognition. Using OpenCV and MadMapper.





```
test_imagenet.py
# USAGE
# python test_imagenet.py --image images/dog_beagle.png

# import the necessary packages
from keras.preprocessing import image as image_utils
from keras.applications.imagenet_utils import decode_predictions
from keras.applications.imagenet_utils import preprocess_input
from keras.applications import VGG16
import numpy as np
import argparse
import cv2

# construct the argument parser and parse the arguments
ap = argparse.ArgumentParser()
ap.add_argument("-i", "--image", required=True,
    help="path to the input image")
args = vars(ap.parse_args())

# load the original image via OpenCV so we can draw on it and display
# it to our screen later
orig = cv2.imread(args["image"])

# load the input image using the Keras helper utility while ensuring
# that the image is resized to 224x224 pixels, the required input
# dimensions for the network -- then convert the PIL image to a
# Numpy array
print("[INFO] loading and preprocessing image...")
image = image_utils.load_img(args["image"], target_size=(224, 224))
image = image_utils.img_to_array(image)

# our image is now represented by a NumPy array of shape (224, 224, 3),
# assuming TensorFlow "channels last" ordering of course, but we need
# to expand the dimensions to be (1, 3, 224, 224) so we can pass it
# through the network -- we'll also preprocess the image by subtracting
# the mean RGB pixel intensity from the ImageNet dataset
image = np.expand_dims(image, axis=0)
image = preprocess_input(image)

# load the VGG16 network pre-trained on the ImageNet dataset
print("[INFO] loading network...")
model = VGG16(weights="imagenet")

# classify the image
print("[INFO] classifying image...")
preds = model.predict(image)
P = decode_predictions(preds)

# loop over the predictions and display the rank-5 predictions +
# probabilities to our terminal
for (i, (imagenetID, label, prob)) in enumerate(P[0]):
    print("{}. {}: {:.2f}%".format(i + 1, label, prob * 100))

# load the image via OpenCV, draw the top prediction on the image,
# and display the image to our screen
orig = cv2.imread(args["image"])
(imagenetID, label, prob) = P[0][0]
cv2.putText(orig, "Label: {}, {:.2f}%".format(label, prob * 100),
    (10, 30), cv2.FONT_HERSHEY_SIMPLEX, 0.8, (0, 255, 0), 2)
cv2.imshow("Classification", orig)
cv2.waitKey(0)
```

OpenCV python library. Setting up a simple program to open up the webcam and calculate the coordinates of the face.

McCahill Mike (2002). -

“You are on a video camera an average of ten times a day. Are you dressed for it?”

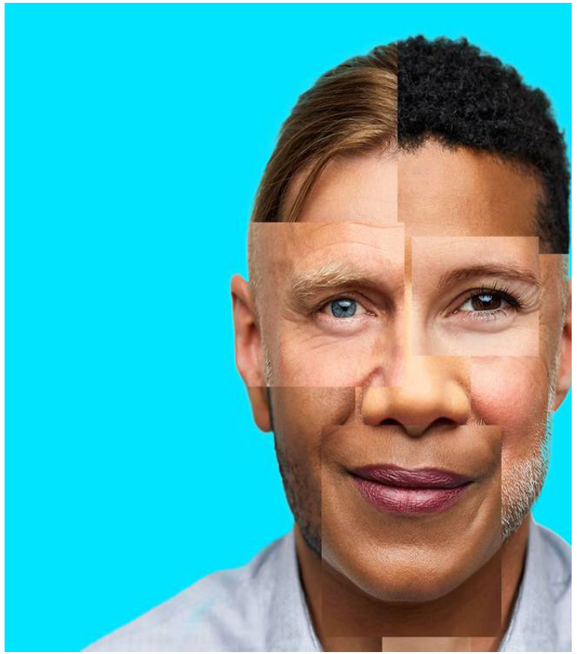
Facial recognition technology (FRT) provides a sophisticated surveillance technique that can be more accurate than the human eye in certain situations like crowded places, surveillance cameras boast real-time face scanning and identification capabilities.

According to the market research done by Mordor Intelligence (2019), the facial recognition market was valued at USD 4.51 billion in 2018 and is expected to reach a value of USD 9.06 billion by 2024, at a CAGR (Compound annual growth rate) of 12.5%, for the forecast period (2019-2024).

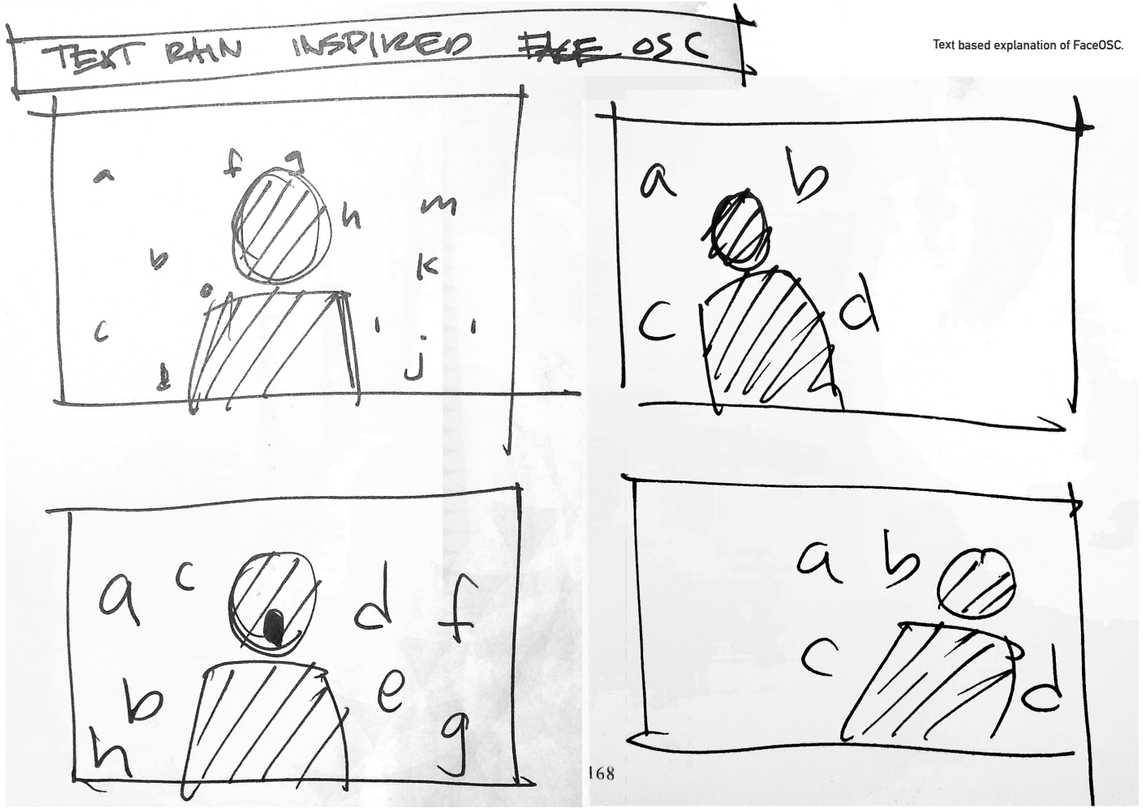
Facial recognition is a really common practice, it is being used in various fields including airports, job interviews, for marketing purposes, unlocking phones and even for social status in China.

With an increase in other sectors including, healthcare, education, workplace and criminal investigations. Facial recognition has been gaining prominence in recent times, owing to the benefits it offers over traditional surveillance techniques, like biometrics.

Governments across the world have been investing significant resources in facial recognition technology, among which, the United States and China are leading adopters.

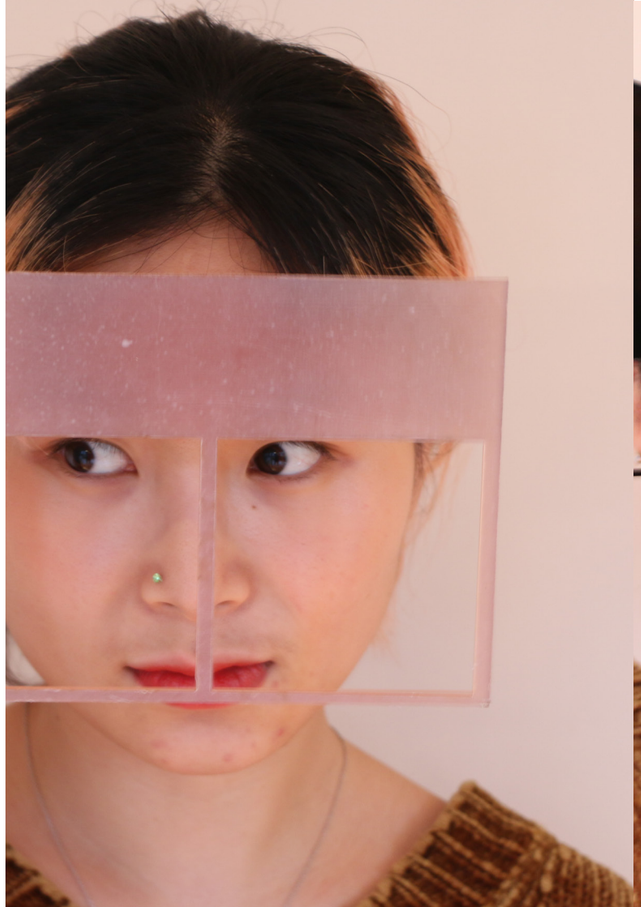


Facial Recognition - www.wired.co.uk



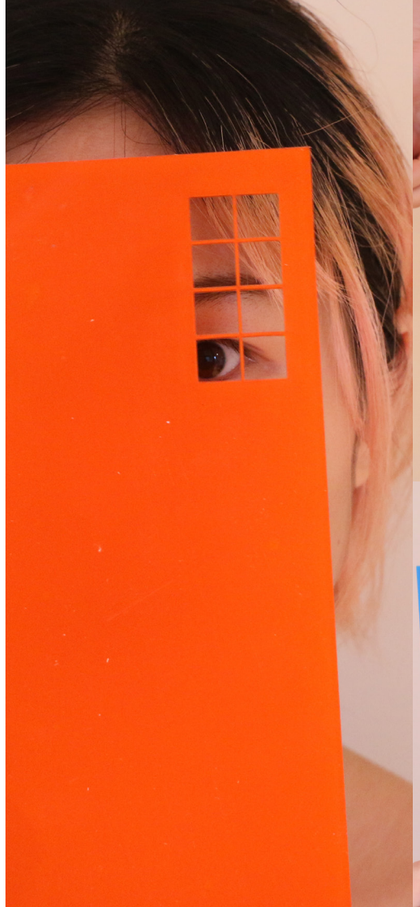
Text based explanation of FaceOSC.

Experimentation using different
objects of various materials.
Trying to find the perfect angle,
object and material, to avoid
OpneCV algorithm.
Model: Ulrica.

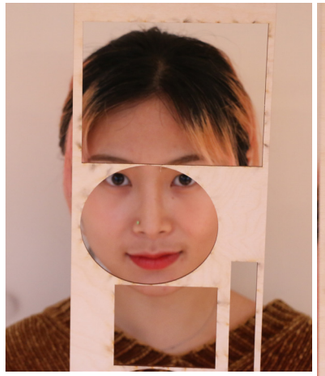


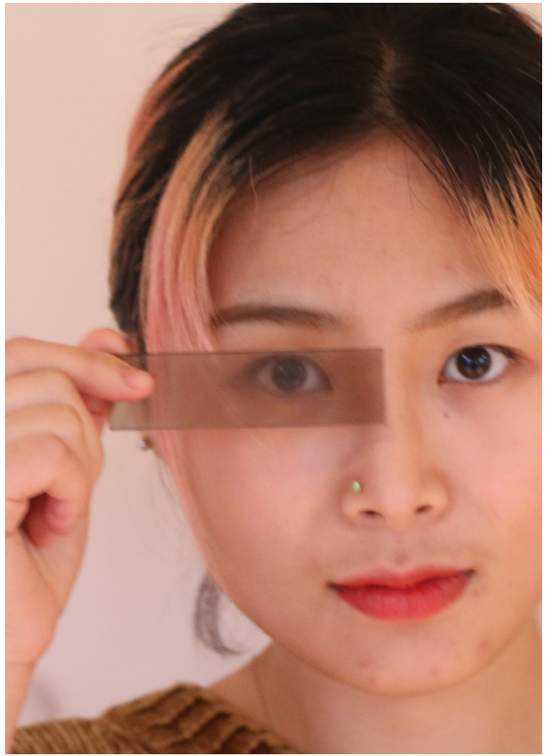
Facial recognition is already in our day to day lives, tagging friends on Facebook, securing homes and phones. Gladstone Nikki (2018) in her article How Facial Recognition Technology Permeated Everyday Life provides her insight and raises a very reasonable concern.

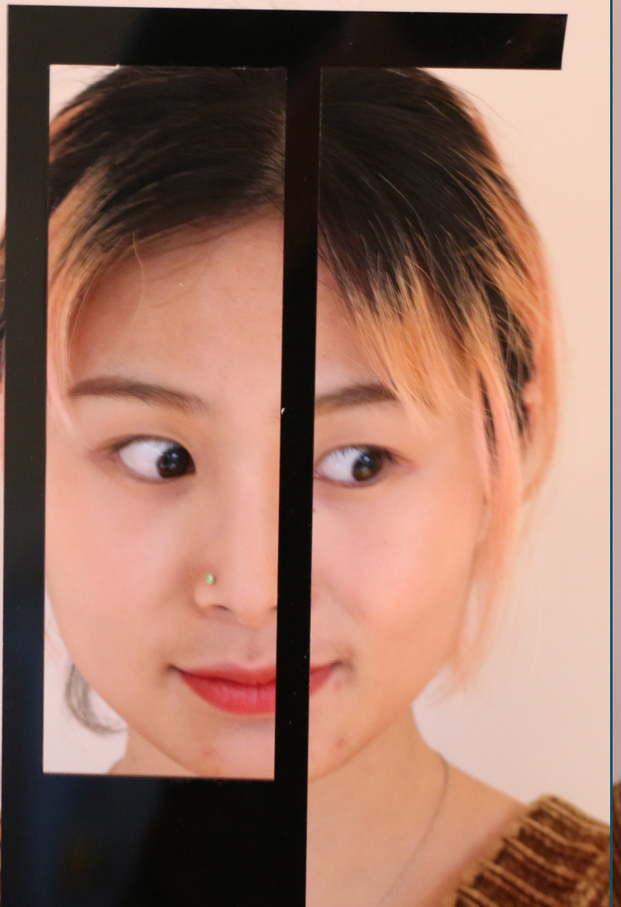
"Facial recognition technology has already permeated our day-to-day activities. It unlocks phones, tags friends on Facebook and secures homes. But personal engagement with a technology doesn't always translate into a full understanding of how that technology collects and uses data."

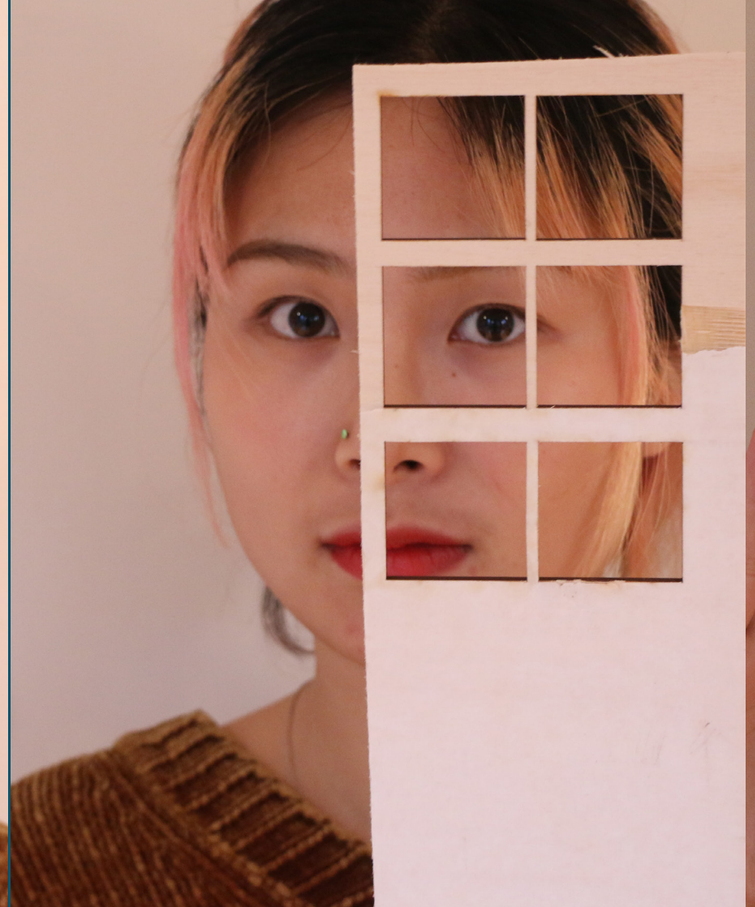


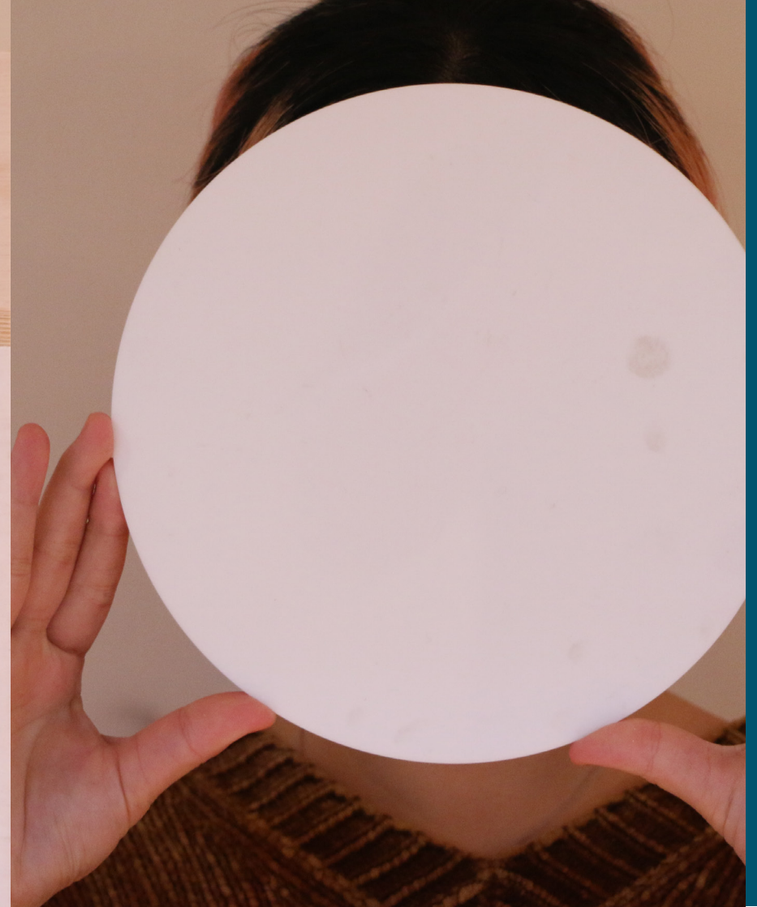
Say cheese! You're being watched.
Facial Recognition technique raises a lot of questions and concerns in people's mind, and at the same time helps people in a lot of ways whilst making their lives easier. Unlocking your phone by just looking at it, doesn't get easier than this, does it? But what exactly is facial recognition? How is it being used? What are the benefits of this technology?











Motivation of this project was seeded into my mind when I visited Grosvenor casino in April 2019 located on Leicester square in London, on the door the security asked me if I have ever visited a Grosvenor casino before and with no memory of ever being there, I said no. After standing there for two minutes, he approached me to inform that I was there in 2014 and showed me a picture of my face. It was exciting, to learn about a technology which is being used to keep track of the people visiting a casino. The ubiquitous use of facial biometrics raises important privacy concerns; particularly problematic are scenarios where a face image is automatically matched against a database without the explicit consent of a person.

With the ease of use comes the concerns about privacy, it was really helpful for the casino to know if a person has been to their facilities before. But what about the person's privacy? The interest of learning more and more about this fascinating piece of technology was really intriguing to me.

As per Navlakha Meera (2019) Eight Of The Ten Most-Surveilled Cities In The World Are In China "A higher number of cameras just barely correlates with a higher safety index and lower crime index. Broadly speaking, more cameras doesn't necessarily result in people feeling safer."

The aim of this project is to visualise the connection between the surveillance cameras with population and their crime rate index.

Ng Lance (2019) shared his insight from a trusted confidential source that, "There are an estimated 176 million CCTV cameras in China today, and a Chinese company's software claims to be able to screen 1.8 billion pictures in three seconds. They also claimed to be able to handle ageing or partially hidden faces with their face matching algorithms."

With everyday use of Facial Recognition increasing by significant numbers in all the fields was a starting point for me for this project.

Talking Cameras! Tottenham Court Road station London,Two camera facing each other.

Contextual background.

In 1966 with Marvin Minsky a young professor at MIT, he decided that the ability to interpret images is called Intelligence. He went ahead and gave one of his under-grad students a task over the summer and requested Gerald Sussman as mentioned by Gonzalez Robbie (2014) Computers Wrote the Caption for This Photograph, and Changed Everything to "spend his summer linking a camera to a computer and letting computer describe what it was".

It was called Summer Vision project, the project was far-fetched in one summer, what I have researched and learnt that smart humans have worked for decades on the computer vision problem and in the late 1990s, there was progress shown in this particular topic. Fast-forwarding to today a computer can recognise anything and anyone in a matter of seconds, but what about the privacy laws?

Barbican Centre: Trevor Paglen
From 'Apple' to 'Anomaly'

Is it still a challenge to ask computer to describe what they see? Learning more on how it works, there are numerous algorithms used for efficiency and are being worked upon to get better results on a daily basis.

Humans tend to learn how to recognise faces from as young as 45 hours. According to Field, T. M., Cohen, D., Garcia, R., & Greenberg, R (1984) experiments and research, at 45-hours old child will be able to distinguish between its mother's face and other faces.

In the 21st century, when there is a smart watch (Apple Watch Series 5), smart enough which enables customers to take an electrocardiogram right from their wrist. It was time that the computer also got smarter in performing functions like recognising faces.

But how does a computer do this? How are we teaching A.I to learn faces and label them? ImageNet was founded - ImageNet is an image database organized according to the WordNet hierarchy (currently only the nouns), in which each node of the hierarchy is depicted by hundreds and thousands of images.

CVDazzle: A technique to avoid facial recognition using make up and patterns.

Ewa Nowak: A designer face mask experiment to avoid the facial recognition.

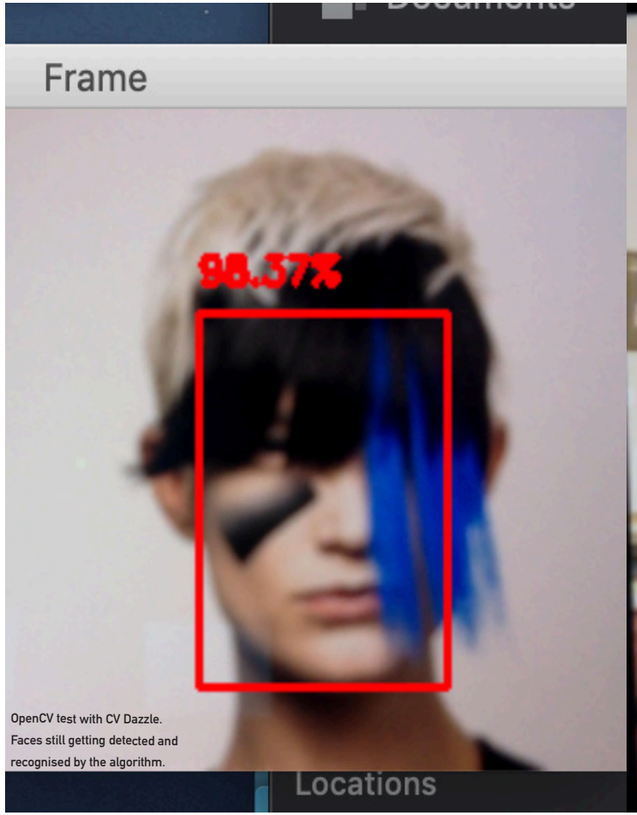
Experimenting with CV Dazzle.
Ewa Nowak and prosthetic mask
to avoid OpenCV algorithm.

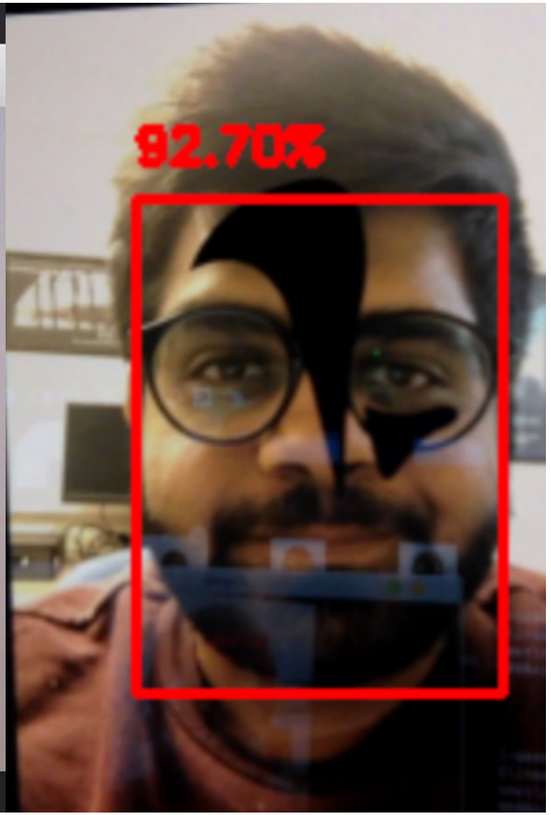
Taking ImageNet as basis, algorithms started teaching a computer about the various different type of images and pictures. You open up a database of pictures which includes faces, objects, things, scenery, different places. With the help of millions and millions of pictures, tell the computer what is a face? How is a face structured in a picture?

At first, things seem straightforward. You're met with apples and oranges, birds, dogs, horses, mountains, clouds, houses, and street signs. But as you probe further into the dataset, people begin to appear: cheerleaders, scuba divers, welders, Boy Scouts, fire walkers, and flower girls. Things get strange:

A photograph of a woman smiling in a bikini is labelled a "slattern, slut, slovenly woman, trollop." A young man drinking beer is categorized as an "alcoholic, alky, dipsomaniac, boozer, lush, soaker, souse." A child wearing sunglasses is classified as a "failure, loser, non-starter, unsuccessful person." You're looking at the "person" category in ImageNet, things start to get a little out of hand, how did we get here?

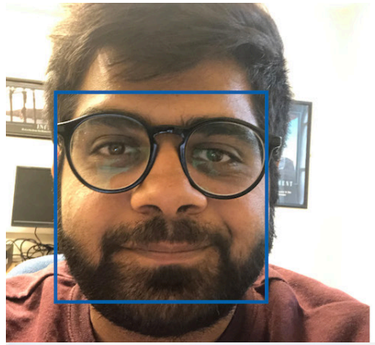
Ewa Nowak mask experiment in use.

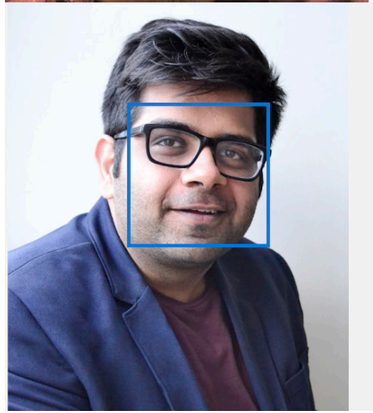




OpenCV test with CV Dazzle. Faces still getting detected and recognised by the algorithm.

36



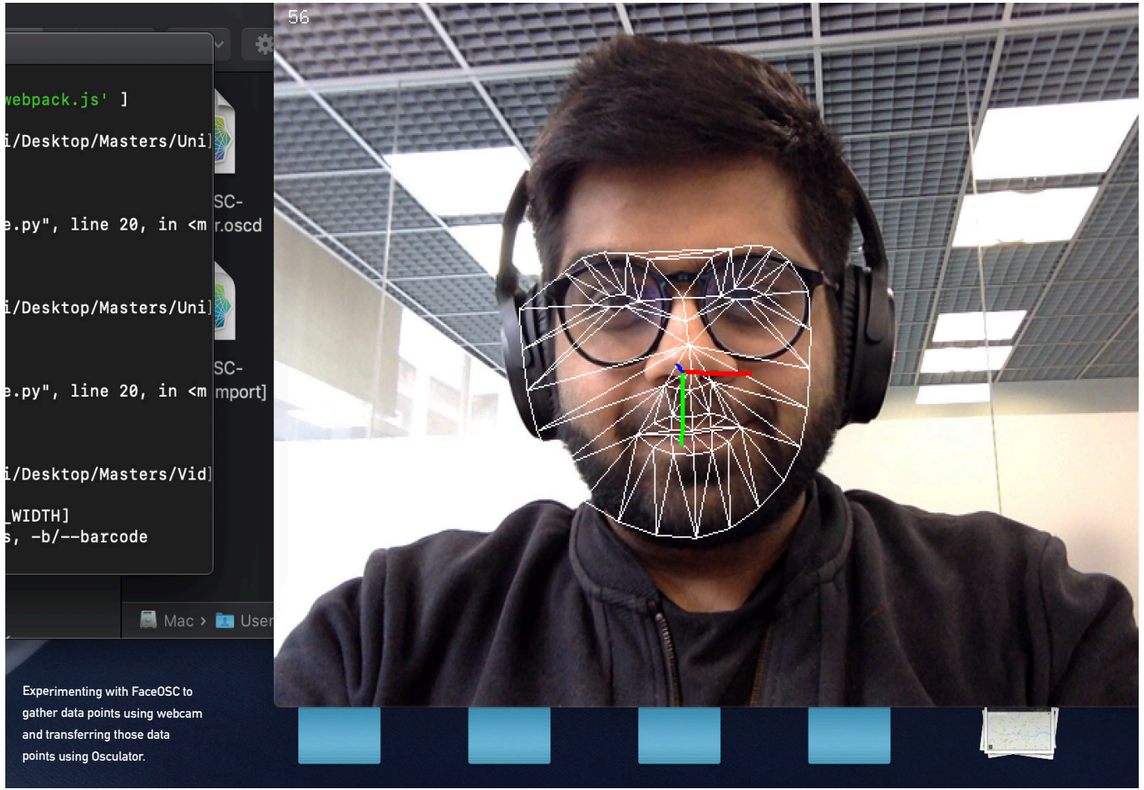



```
[
 {
   "faceRectangle": {
     "top": 1055,
     "left": 449,
     "width": 1278,
     "height": 1278
   },
   "faceAttributes": {
     "emotion": {
       "anger": 0.0,
       "contempt": 0.018,
       "disgust": 0.0,
       "fear": 0.0,
       "happiness": 0.608,
       "neutral": 0.373,
       "sadness": 0.0,
       "surprise": 0.0
     }
       },
       {
         "color": "gray",
         "confidence": 0.79
       },
       {
         "color": "brown",
         "confidence": 0.74
       },
       {
         "color": "other",
         "confidence": 0.46
       },
       {
         "color": "blond",
         "confidence": 0.03
       },
       {
         "color": "red",
         "confidence": 0.03
       }
     ]
```


37

Experimenting with Microsoft API using same person with different images to check and compare the results.

FEATURE NAME:	VALUE
Objects	[{ "rectangle": { "x": 14, "y": 310, "w": 751, "h": 705 }, "object": "person", "confidence": 0.921 }]
Tags	[{ "name": "person", "confidence": 0.9982785 }, { "name": "man", "confidence": 0.986790836 }, { "name": "wall", "confidence": 0.9772988 }, { "name": "indoor", "confidence": 0.964628041 }]
Description	{ "tags": ["person", "man", "indoor", "glasses", "table", "food", "sitting", "looking", "front", "holding", "camera", "restaurant", "wearing", "shirt", "smiling", "plate", "eating", "white", "standing", "laptop", "young", "people", "large", "room"], "captions": [{ "text": "a man wearing glasses and smiling at the camera", "confidence": 0.9435803 }] }

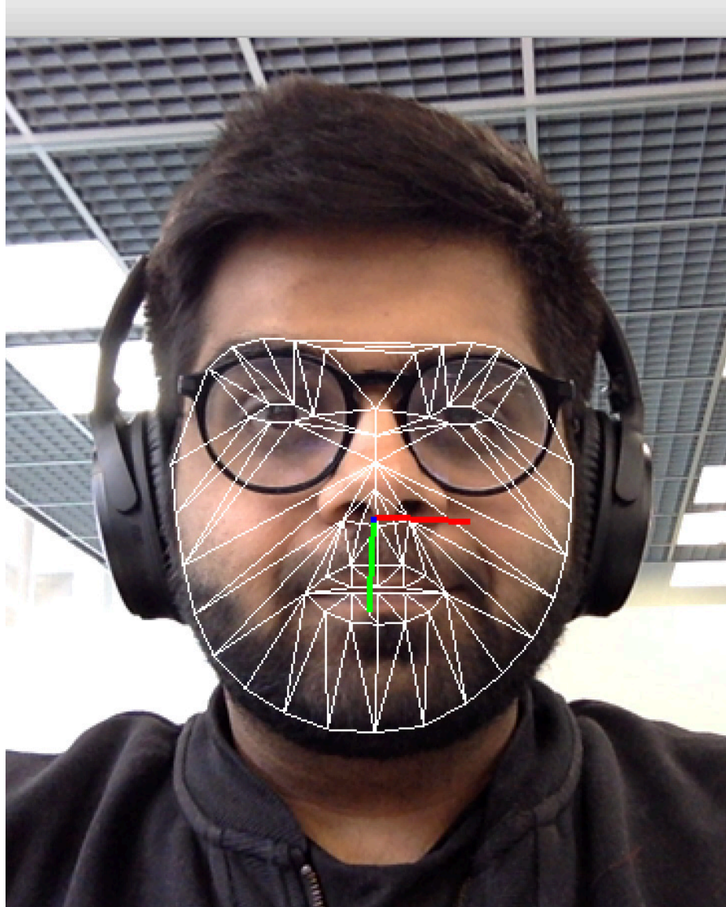


Experimenting with FaceOSC to gather data points using webcam and transferring those data points using Osculator.

Technology has moved light years since, Marvin started this research, now computers are scanning our faces whilst we're not even aware of what is happening.

Are consumers aware of being recognised and detected using their faces? Or as said by Gladstone Nikki (2018) How Facial Recognition Technology Permeated Everyday Life, "Facial recognition technology's undetectable nature makes it easy to abuse.

To acquire a fingerprint or conduct an iris scan, there's a degree of involvement required from the person whose information is being collected. Facial features, on the other hand, can be collected from a distance without direct participation, meaning the whole process can occur without the individual's knowledge — and importantly, consent."



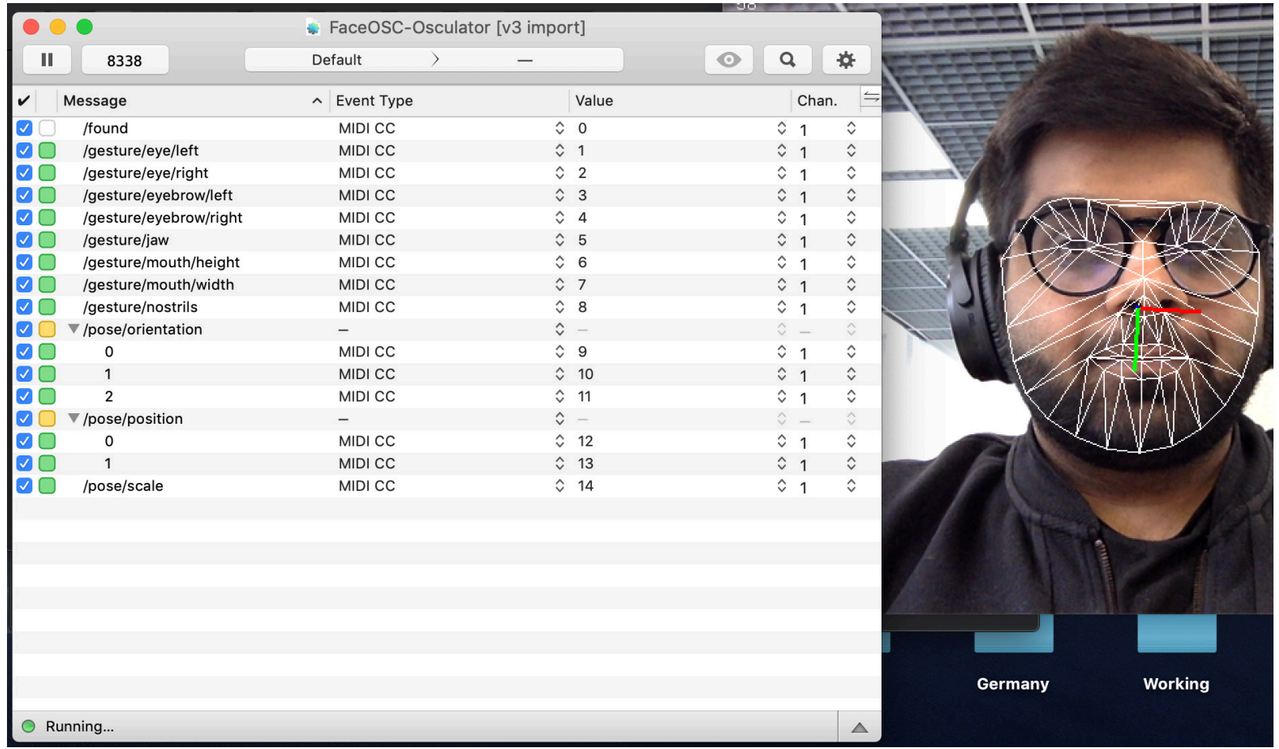
Capturing live data points, using Osculator. Transfering those data points to track movement.

Sample Ian (2019) What is facial recognition - and how sinister is it? Mentioned his key insights about facial recognition with some statistics from US National Institute of Standards and Technology (Nist).

Reported that between 2014 and 2018 facial recognition systems got 20 times better at finding a match in a database of 12m portrait photos. The failure rate fell from 4% to 0.2% over the period, a massive gain in accuracy that was largely down to deep neural networks. Nist says the networks have driven "an industrial revolution" in facial recognition.

Facial recognition is a piece of technology which is being developed upon as you're reading this piece of text, there are constantly new changes in the field every day.

Varying from DeepFakes (which is used to. generate fake news videos and images of people) to its use in urban space like London King's Cross.



Osculator User Interface showing various different data types being collected.

Research Methods

Research methods for this project includes going around London, finding a lot of surveillance cameras and understanding their placement.

How efficiently and effectively are they placed to capture a lot of people from various angles.

Visiting barbican centre to see the Trevor Paglen from 'Apple' to 'Anomaly', which explains how the ImageNet algorithm works, it explores various different topics of none related things, and how algorithms labels.

The primary research includes, writing code in Python and FaceOSC using jupyter notebooks, to explore various different methods on how to avoid facial recognition.

Testing on myself and a friend using variety of materials to cover the face still getting detected as the computer learns the structure of different faces. Capturing gestures using FaceOSC and converting them into data points.

Surveillance is the business model of the Internet.

- Bruce Schneier, American cryptographer

South Kensington underground station, London

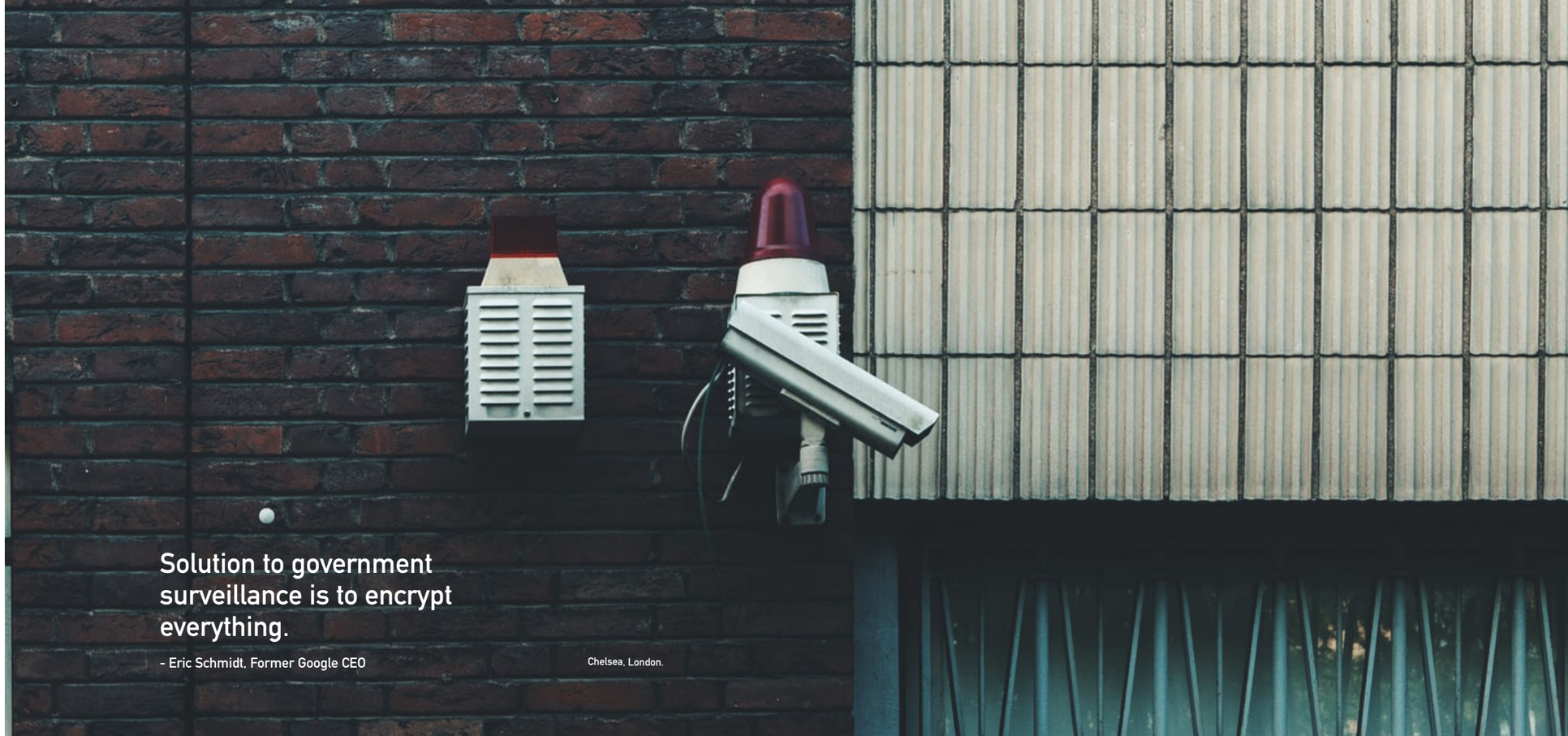
Secondary or desk researching, focusing on collecting information about, how the facial recognition technology works? How it is changing?

How it is being used? Effectively moving the project and research towards the social and personal implications of the facial recognition technology.

Exploring the surveillance data of various countries including US, China, UK and India. Connecting the dots in data and finding the stories in between the surveillance data and population geographically.

Getting hands on with making a facial recognition system is not hard, it is surprisingly simple and with OpenCV (python library) which is open and free, more and more people are getting experimenting with the technology. Starting with the applications of facial recognition with simple explanation on how it works! What other examples are there?

The computer has to learn what a face is. This can be done by training an algorithm, usually a deep neural network, on a huge number of photos that have faces. Each time the algorithm is shown an image, it tries to find where the face is. The network will be horrible at first. But if this is done multiple times, the algorithm improves and eventually masters the art of spotting a face.

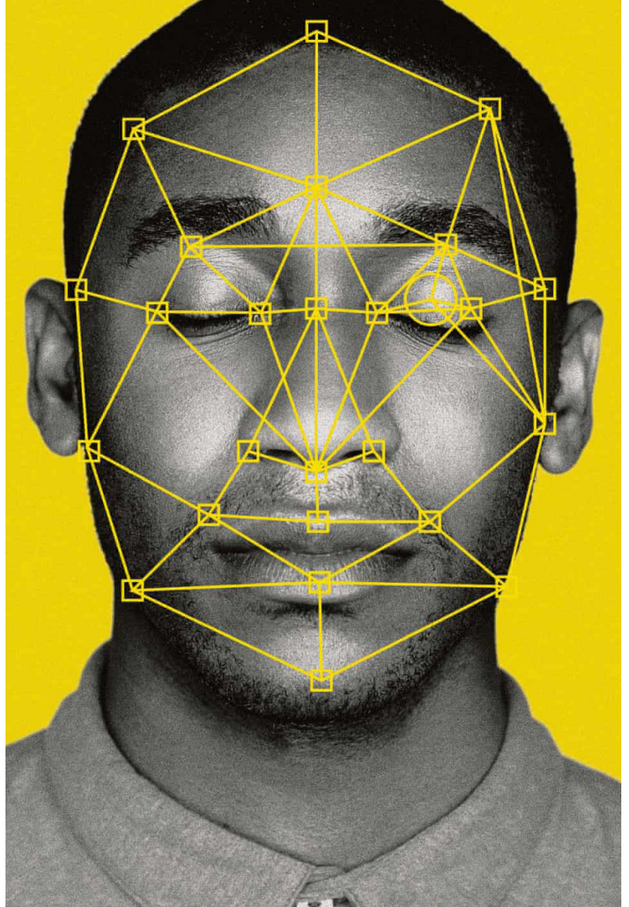


London College of Communication Entrance. Elephant and Castle, London.

Basic Facial Recognition: For Snapchat, Instagram and Animoji (Apple's emojis using front camera and facial detection). Scans the live feed of the camera for the defining features of a face like, eyes, mouth, ears, nose and a mouth.

Moving ahead after detecting the basic features, the algorithm confirms the face and then determines the extra features like, direction of the face and if the mouth it open or closed for additional effects.

It is very easy to trick this tech, as it is not looking for depth or 3D mapping the face. Very basic just scanning the image/video feed for basic face features, with a printed image of a person, it can be tricked into thinking it is a face and will add filters to the image.



Face Recognition: www.guardian.co.uk

Face Identification (Face ID): Used by latest Apple iPhones (X, XS, 11) and various other companies in their new addition of smart phones including Google Pixel 4.

It works by using infrared projectors and creating a 3D true depth face data by projecting infrared dots on the face. Which returns with an infrared data map of the face, and results in one of the most secure facial recognition systems.

It is very hard to trick this system as it tracks significant changes in users appearance, including make-up, facial hair and also works in total darkness. It takes less than a second for the whole process to happen.

Face Recognition:
www.guardian.co.uk

Surveillance: The system used in China is an example of facial recognition surveillance. It is used for racial profiling, and social status. "When a resident of Anxi village in China's southwest Sichuan province set fire to a pile of rubbish two years ago, a loudspeaker barked his name and ordered him to put the blaze out. He extinguished the flames and scuttled away."

Everyone in the village knew, who was the culprit, he was captured on the 16 huge screens in the surveillance office of the village. China uses one of the world's best facial recognition system, it tracks users even when facing down, or side profiles. It is almost impossible to avoid the system, whilst you are in China.

CCTV Camera.
Holborn station, London

"General Data Protection Regulation (GDPR)" for European Member States does address biometric data and represents a major step forward for data protection and privacy with a true international impact."

The EU data privacy law defines biometric data as "special categories of personal data" and prohibits its "processing". Gather this information online (Biometric data and data protection regulations (GDPR and CCPA).

More precisely as mentioned by Information Commission's Office (ico), biometric data are "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data".

50

However fast regulation moves, technology moves faster. Especially as far as data is concerned.

- Elizabeth Denham, CBE is the UK Information Commissioner

These regulations help and protect all the UK and long-term EU residents from their data being shared with the third parties without their consent. As explained by ICO (2018) Guide to the General Data Protection Regulation report the laws are divided into 7 parts covering all the major concerns regarding the biometric data:

51

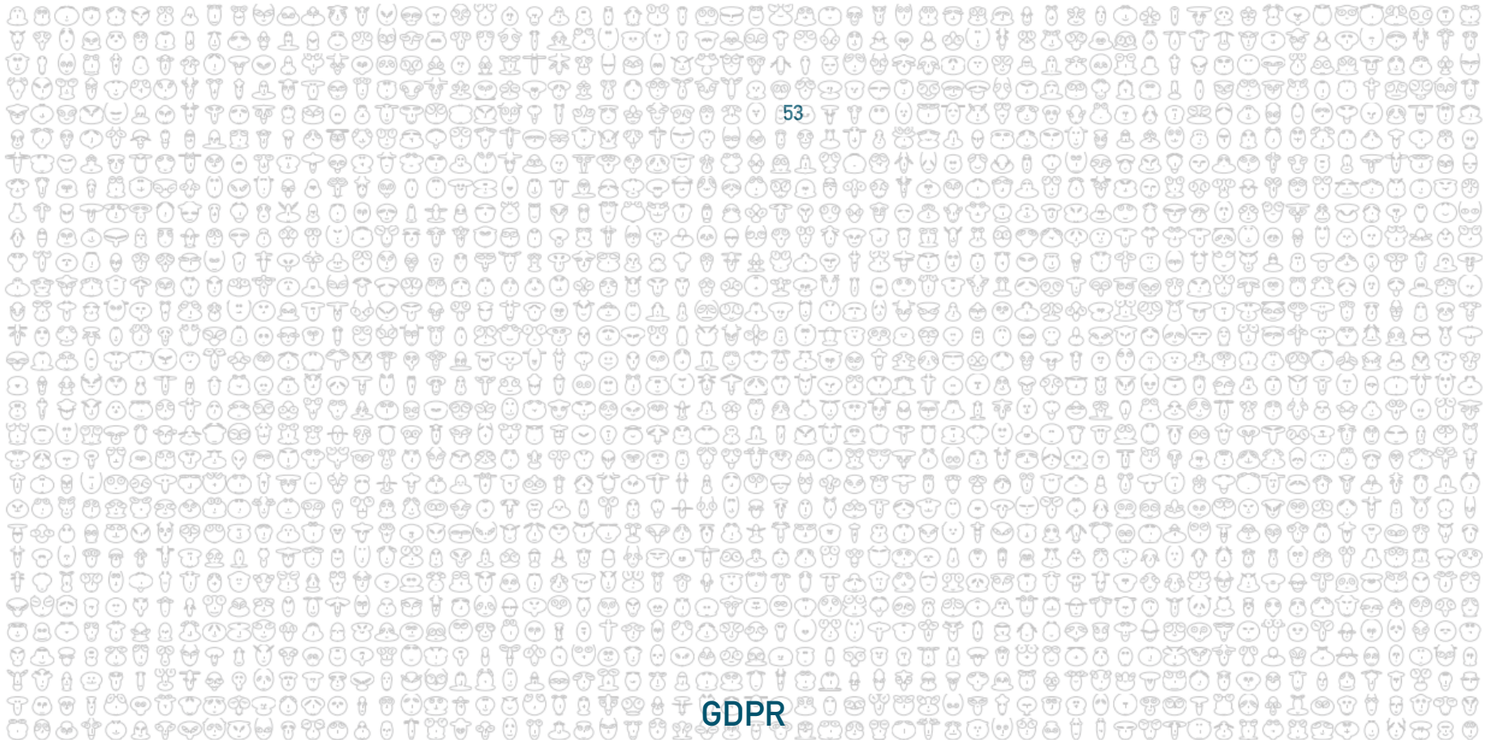
Everyone has a say!

Consent: In obtaining consent for the data use, companies cannot use indecipherable terms and conditions and it should always come with easy options of withdrawing the consent.

Breach Notification: In the event of a data breach, the consumer should be informed of any risk within 72 hours.

Right to Access: Consumers have the right to ask for all the data stored by the companies concerning them, and the companies have to provide an electronic copy for free of cost.

Right to be forgotten: When the data collected is not being used or has met it's purpose, the consumer has the right to request deletion of its data from companies data servers.



GDPR

Chernoff Faces:
www.flowingdata.com

Data portability: This allows users to use their biometric data from one application to another. Like for example, using Face ID or Touch ID on iPhones not only for unlocking the device, even for bank payments and movie ticket payments.

Privacy by design: The companies are supposed to include all the privacy and guidelines while making their products.

Data Protection Officers: Professionally qualified officers must be appointed in all the public and large organisations (>250 employees).

Camera, Elephant and Castle, London.

There are more than 5 incidents in last year (2018) where people were under surveillance without their consent in UK. Including cities like, Birmingham,

Manchester, Liverpool, Sheffield and last but not the least London. Carlo Silkie (2019), Big Brother Watch's director, described the rollout as an "epidemic of facial recognition in the UK". She said:

"The collusion between police and private companies in building these surveillance nets around popular spaces is deeply disturbing. Facial recognition is the perfect tool of oppression and the widespread use we've found indicates we're facing a privacy emergency."

According to the insight analysis by Comparitech, Bischoff Paul's (2019)
The world's most-surveilled cities provides information in August (2019) that London (627,707 cameras for 9,176,530 people = 68.40 cameras per 1,000 people) has the highest number of surveillance cameras of any city outside of China. And estimates by Big Brother Watch suggest Britain has the second-most surveillance cameras per capita of any country in the world.

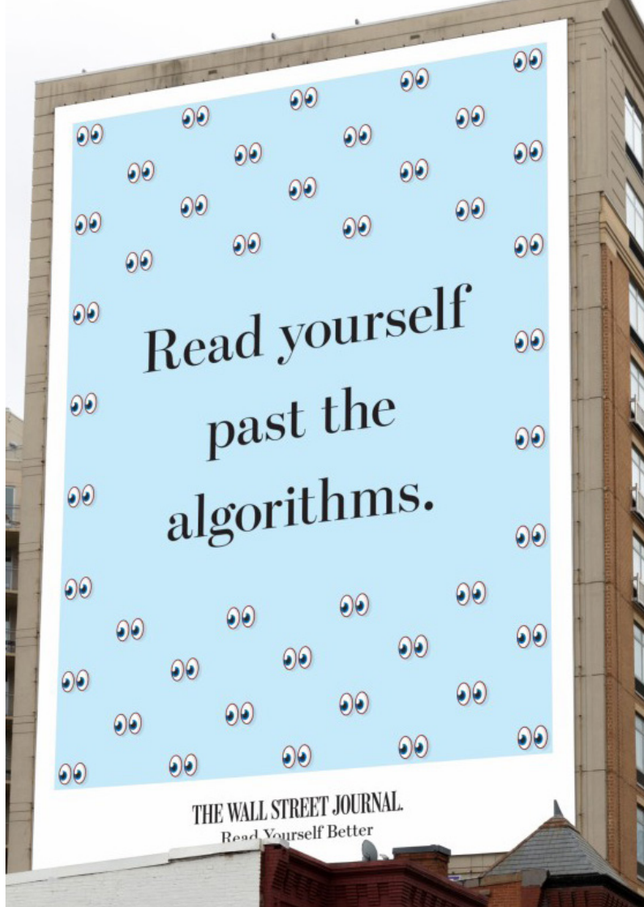
Learning more about UK's population's opinion about the Facial Recognition system with Ada Lovelace Institute (2019) "Public Attitude Towards Facial Recognition", which includes some important findings about the state of Facial Recognition technology in the country and what do people think about it.

"Awareness of facial recognition technology is high, but knowledge about it is low", This direct quote from the report Ada Lovelace Institute (2019) Public Attitude Towards Facial Recognition. Clearly explains the situation of Facial Recognition tech in people's mind.

Getting deeper into the report we can extract that people are making assumptions about the facial recognition technology, around 24% people who are answering the questions in the survey conducted by Ada Lovelace institute (2019),

Question the reliability and accuracy of the technology and assume that it is biased towards different race or gender whilst it is used by Police and on the other hand only 18% think it's accurate.

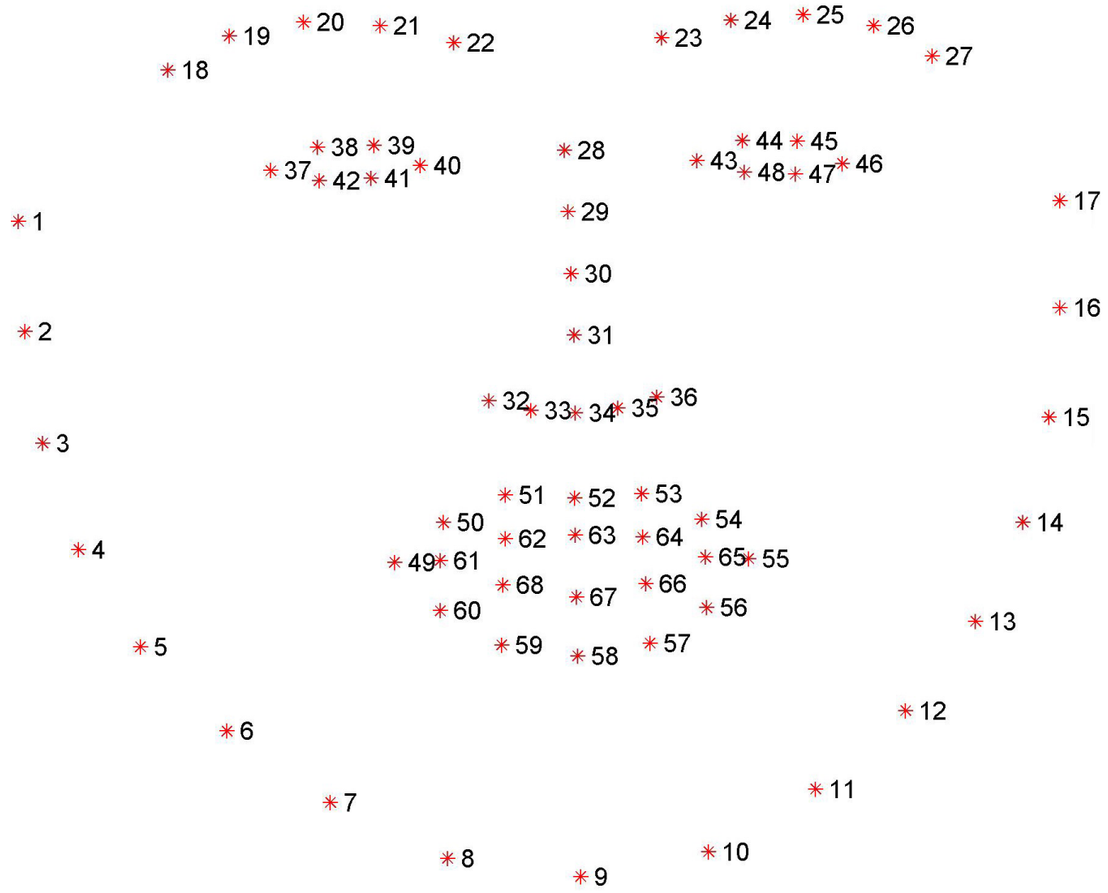
One of the top concerns of the people who appeared for the survey was "Consent".



South Kensington Station, London.

Almost half of the people (46%) filling the survey agreed to have an option to opt-out of Facial Recognition, and only 28% of people disagreed that there should be an option. Most survey respondents from different ethnic groups including Black, Asians and other minority ethnicity were keener on having the opt-out feature than compared to the majority.

Report also clearly states that "People fear the normalisation of surveillance but will accept facial recognition technology when there is a clear public benefit".



Data points collected and projected using Osculator. Creating a face image.

People agree to use the technology for unlocking their phones but are not very keen in moving towards a tracked environment. The report has a mixed emotion from the people for the facial recognition technology, it is not definite how people think about the tech, it is still hard to come to a conclusion on, how people actually view the facial recognition tech?

Bethnal Green, Underground Station, London.

Imagine that this is your daily life: While on your way to work or on an errand, every 100 meters you pass a police blockhouse. Video cameras on street corners and lamp posts recognize your face and track your movements.

At multiple checkpoints, police officers scan your ID card, your irises and the contents of your phone. At the supermarket or the bank, you are scanned again, your bags are X-rayed and an officer runs a wand over your body.

Avoidance?

Use of facial recognition tech is on the rise, but how do you get away from it? There are vast amount of experiments done globally on how to avoid the facial recognition technology.

Some of them include 3D-printed face masks, makeup, infrared and glowing lights on the glasses, and complex patterns are being experimented with to dodge the tech. Like for example the project by JING-CAI LIU's "wearable face projector" keeping in mind which she did about the privacy constraints of facial recognition.

Is a global scale project which is being used to avoid the tech and protect the privacy of consumers? One more widely used example is CV Dazzle, a camouflaged make up technique which helps in not getting the face detected as it distorts facial structure which is tracked by OpenCV (most commonly used facial detection algorithm).

Hounslow, London.

Elephant and Castle, London.

According to Daily Mail (Police arrest passenger who boarded plane in Hong Kong as an old man in flat cap and arrived in Canada a young Asian refugee, 2011), a real case was reported in which a young person from Hong Kong boarded a plane to Canada disguised as an old man with a flat hat [Mail 2015].

This person used a silicon face and neck mask to successfully fool the border c ontrol authorities.

Elise Thomas (2019) How to hack your face to dodge the rise of facial recognition tech for Wired Technologies mentions that for fooling FR can be roughly divided into two categories: occlusion or confusion.

Thomas's critical "Occlusion techniques work by physically hiding facial features so the camera simply can't see them. How successful these methods are will depend on which bits of your face are hidden and how well hidden they are." Occlusion is something which is used by people in various ways, like a "Burkha" will be able to protect your identity as it covers your mouth and nose but on the other hand a "balaclava" will not cause an occlusion while protecting your identity as it reveals the most important parts of your face (nose, eyes and mouth)

Transport for London red bus.

Occlusion can only be achieved by covering the vital parts of the face, on the other hand confusion, making the FR system believe that is not looking at a face, there are 14 vital key points which an Facial Recognition system reads when looking for a face, or as Ryan (co-founder at CV dazzle) states "If you're attacking the facial detection stage, you could try and break up the lines of your face to try and stop it from being detected by the system in the first places,".

While personally experimenting CV dazzle technique with a simple python OpenCV script using my MacBook 2013 FaceTime camera, it failed miserably and repetitively. Are these techniques actually useful? Are they helping anyone? Has anyone ever actually used it? How successful were they?

According to the Ada Lovelace Beyond face value: public attitudes to facial recognition technology report there are a lot of social and ethical concerns over the facial recognition. People are not comfortable with Facial Recognition tech being used in the private commercial sector and with the increase in the use of technology, people have started to voice their concerns.

A company called "Big Brother Watch" which exposes and challenges all the threats to the privacy of UK residents and the use of their data. According to Big Brother Watch (2019) website, their work description states, "They campaign to protect freedom in parliament and through the courts while seeking to educate and empower the public."

Concerns.
Concerns.

Software: Atom
Code: Open CV algorithm

```
parse_cmd(int argc, const char** argv,
    char* ftFile,char* conFile,char* triFile,
    bool &fcheck,double &scale,int &fpd)

int i; fcheck = false; scale = 1; fpd = -1;
for(i = 1; i < argc; i++){
 if((std::strcmp(argv[i],"-?") == 0) ||
   (std::strcmp(argv[i],"--help") == 0)){
  std::cout << "track_face:- Written by Jason Saragih 2010
  << "Performs automatic face tracking" << std::endl << std
  << "#" << std::endl
  << "# usage: ./face_tracker [options]" << std::endl
  << "#" << std::endl << std::endl
  << "Arguments:" << std::endl
  << "-m <string> -> Tracker model (default: ../model/face7
  << std::endl
  << "-c <string> -> Connectivity (default: ../model/face.c
  << std::endl
  << "-t <string> -> Triangulation (default: ../model/face.
  << std::endl
  << "-s <double> -> Image scaling (default: 1)" << std::en
  << "-d <int>    -> Frames/detections (default: -1)" << st
  << "--check     -> Check for failure" << std::endl;
  return -1;
 }
```

CCTV camera:
www.unsplash.com

Big Brother Watch recently released a report (2018) called "Face-Off: The lawless growth of Facial recognition in UK policing", the report focuses on how Leicestershire Police, South Wales Police and the Metropolitan Police have deployed this technology at shopping centres, festivals, sports events, concerts, community event.

One of the incidents which took place where the police used Facial Recognition technology to keep innocent people with mental health issues away from a political public event. Big Brother Watch using their information-based investigation which involves requesting information from various offices of government for the data, which is legally available to every UK resident.

Big Brother Watch involves over 50 requests for information claims that 95% of matches which police get using Facial Recognition are incorrect and are innocent people. "The Metropolitan Police has the worst record, with less than 2% accuracy of its automated facial recognition 'matches' and over 98% of matches wrongly identifying innocent members of the public."

Big brother watch is trying to get these numbers to people and they seek awareness on the topic, which I believe is nice way to approach a topic which has a lot of concerns regarding privacy, GDPR, ethical and social implications.`

Under observation, we act less free, which means we effectively are less free. - Edward Snowden, Former CIA employee

Getting to a conclusion about concerns on the basis of Big Brother Watch (2018) Face-Off: The lawless growth of Facial recognition in UK policing, the title itself is expressing the negative approach to the concerns.

On the contrary the report by Ada Lovelace institute (2019) states, 65% of people disagree with UK's government in future banning all kind of Facial Recognition systems.

People want Facial Recognition systems to be used but in a healthy manner and not getting tracked for all their movements.

I believe the facial recognition technology is very useful if used whilst following all the rules and guidelines.

It not only helps the government of the using country. It even helps the consumers in vast number of ways.

Big Brother Watch involves over 50 requests for information claims that 95% of matches which police get using Facial Recognition are incorrect and are innocent people. "The Metropolitan Police has the worst record, with less than 2% accuracy of its automated facial recognition 'matches' and over 98% of matches wrongly identifying innocent members of the public."

Big brother watch is trying to get these numbers to people and they seek awareness on the topic, which I believe is nice way to approach a topic which has a lot of concerns regarding privacy, GDPR, ethical and social implications.`

Russel Square underground station, London

There is no legislation regulating the use of CCTV cameras with facial recognition - Nick Hurd, Minister for Policing, United Kingdom

The Law.

In Britain there is no law that gives the police the power to use facial recognition and no government policy on its use. This has led to what Paul Wiles, the Biometrics commissioner, calls a chaotic situation with the police deciding for themselves where and when it is appropriate to use facial recognition and what happens to the images the cameras capture.

The lack of a legal basis or indeed parliamentary scrutiny poses serious concerns about the silent erosion of human rights. It is highly questionable whether the use of automated facial recognition with public surveillance cameras, scanning and biometrically analysing every passer-by's face, and enabling authorities to identify and track citizens without their knowledge, is compatible with fundamental human rights – in particular, the rights to a private life and to freedom of expression.

The necessity of such biometric surveillance is highly questionable, and inherently indiscriminate scanning appears to be plainly disproportionate. As it stands, the risk that automated facial recognition is fundamentally incompatible with people's rights under the Human Rights Act 1998 is yet to be considered.

Hyde Park underground station, London

Looking facial recognition systems from, a legal and ethical perspective there are three major concerns which directly violate some of the existing legislative laws in most countries : discrimination, privacy, and democratic freedom.

There are no direct laws affecting Facial Recognition systems, but there are certain rules against discrimination, if a certain algorithm or practice is found guilty of discrimination it can legally be held up in court.

There are rules which are made by the government to protect citizens from the over and mis use of the technology, according to the UK privacy act (2018), “If your premises, event or application uses facial recognition technology, it’s critical that you ensure your users and customers know it does.

Doing so helps to inform others that such technologies are in place. It also allows those who visit or use your facilities or technology to decide if they wish to continue doing so.” It is called “Providing Notice”.

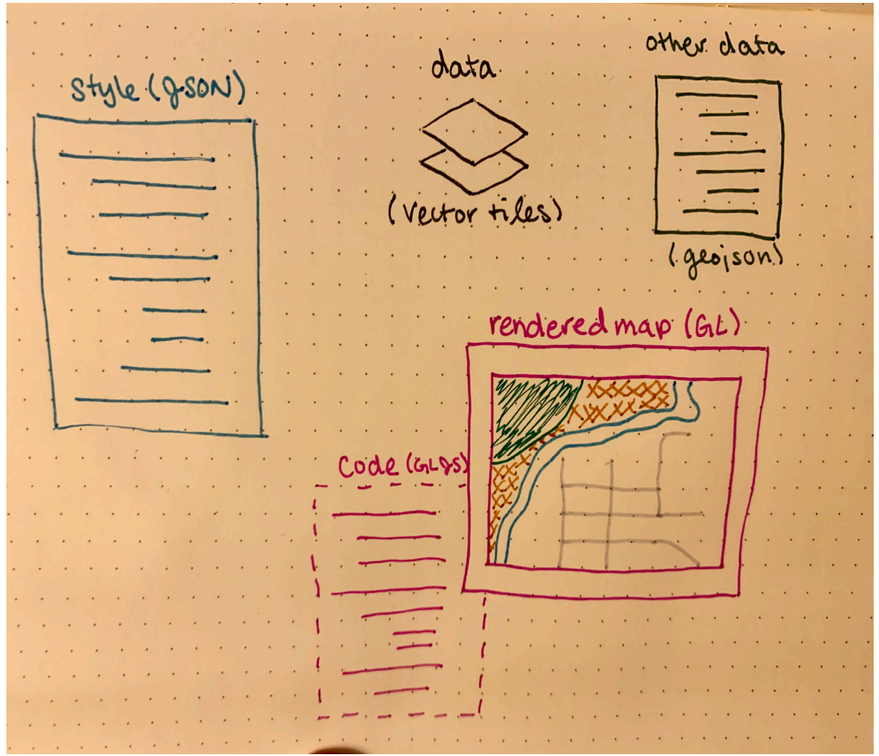
Keeping in mind all the constraints and concerns of using the technology, I will be doing most of the experiments on myself, with various algorithms and techniques to reach the desired outcome.

Design Development

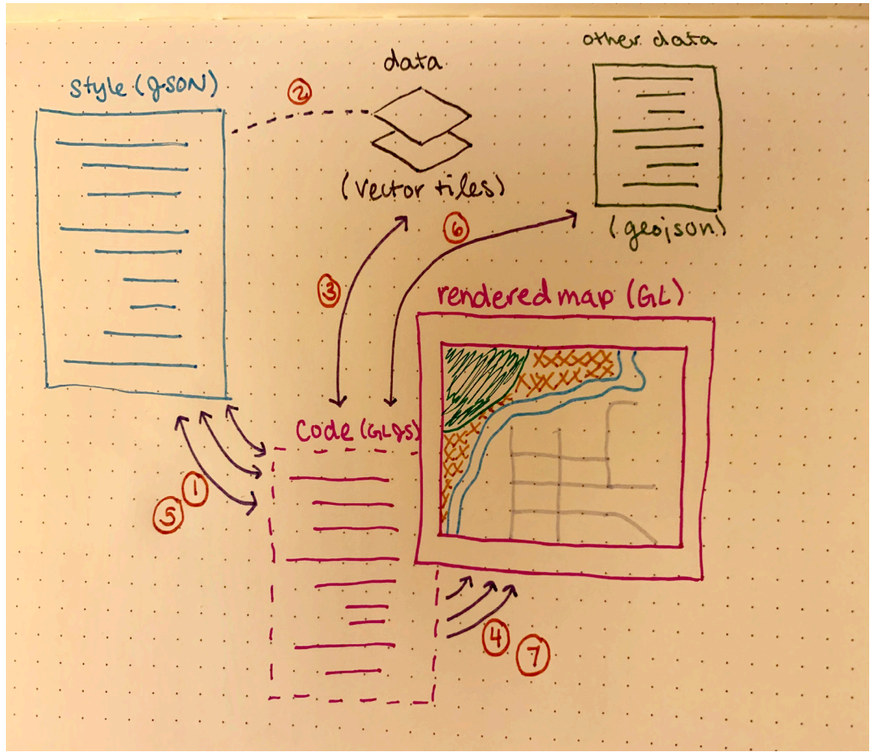
Starting to learn more about the technology of Face ID in my current phone (iPhone X), and was very intrigued how can such a small device recognise a face in less than a second and it is considered to be secure enough to do payments?

Starting to wonder if it was really as secure as they claim it to be? Turns out it is and it always was, Face ID is 25% more secure than Touch ID (apple.com).

Realising on how the idea will turn into a project, I started moving ahead with various different kinds of fields in the topic, like racial bias, deepfakes, surveillance, privacy, laws, concerns. With the increase in surveillance and the cameras all around us, it struck me as an idea. To actually research and find out how effective are the cameras and what are they actually being used for, if not for safety?



Anatomy of how an interactive map works using Javascript and GeoJson.



Working model explaining with arrows, how the data and code is moving.

Secondary or desk research to find answers to these questions, was really helpful and I started experimenting to find the right answers, instead of believing everything I read on the internet.

Experimenting started from a very basic python script which detects faces in the live video stream using my MacBook pro 2013 facetime camera. It was a good starting point for me to learn how the face detection actually works and how is it being used. It was really basic, but even after it being so basic products like CV dazzle were not very helpful in achieving the goal. I particularly chose this system as it was listed by StackOverFlow as the most commonly used system.

After a series of experiments with various different types of materials and techniques,like printing faces to confuse the AI, facial masks, projecting face on a face, and projecting face. There was no success in breaking the system from recognising the user.

Using the more successful approach to the problem by covering the face! Protecting the ID and beating the algorithm with abstract shapes and pieces, which are not very popular and useful but were successful in breaking the algorithm.

The real challenge was to use abstract shapes and pieces and convert them into something meaningful which can be used for real life scenarios and can actually help people in protecting their identities.

Dodging was an option but finding out the global impact of surveillance towards the end of the project was my goal. Designed a complete interactive map using JavaScript, leafletjs. To find the stories behind the cameras around the world. Which country is moving in which direction with the surveillance, and how fast are they moving?

Experimenting with various different kinds of maps, with surveillance data.

Imagine that this is your daily life: While on your way to work or on an errand, every 100 meters you pass a police blockhouse. Video cameras on street corners and lamp posts recognize your face and track your movements.

At multiple checkpoints, police officers scan your ID card, your irises and the contents of your phone. At the supermarket or the bank, you are scanned again, your bags are X-rayed and an officer runs a wand over your body.

World Map experiment.

All of this is now done with the surveillance cameras around us, as mentioned by Millward James A (2018) What It's Like to Live in a Surveillance State, "This personal information, along with your biometric data, resides in a database tied to your ID number.

The system crunches all of this into a composite score that ranks you as "safe," "normal" or "unsafe". Based on those categories, you may or may not be allowed to visit a museum, pass through certain neighbourhoods, go to the mall, check into a hotel, rent an apartment, apply for a job or buy a train ticket."

The audience of this project are the people who would like to explore, the surveillance in their cities. With the help of a simple map.

To explain how the surveillance system is tied to our daily lives, I use a very commonly used approach. Which is through a world map. Keeping the things simple and plain.

I use JavaScript Library Leaflet, which helps in adding interactive features to the map and is most commonly used with OpenStreetMap, which give the structure to the whole project.

Getting the outline and structure from the OpenStreeMap gives the ability to play with the project using CSS. I cleaned the data using python and converted it into a GeoJson file, which saves the data in geographic manner with latitude and longitude of all the places.

The outcome is hosted on a local server for now, the additional steps will be to host it on an online server and tie it with the data directly. So the map gets updated automatically as the data changes on the server.

You can filter the data in map using various fields and explore, the surveillance of your city and how many cameras are there per person in various places around the globe.

Experimenting with data and focusing on data points in United Kingdom.

If you've got something to be worried about, you should probably be worried. - Devlin Hannah Science Correspondent for The Guardian

Critical Rationale.

Surveillance is at its peak and we have seen the numbers to prove it. This project starts with asking questions about facial recognition technology. Explains how different type of facial recognition works and it's uses.

Moving ahead the project also sheds some light on how the facial recognition can be avoided in two different ways occlusion or confusion. The different ways are discussed with various examples and experimented using multiple algorithms. surveillance.

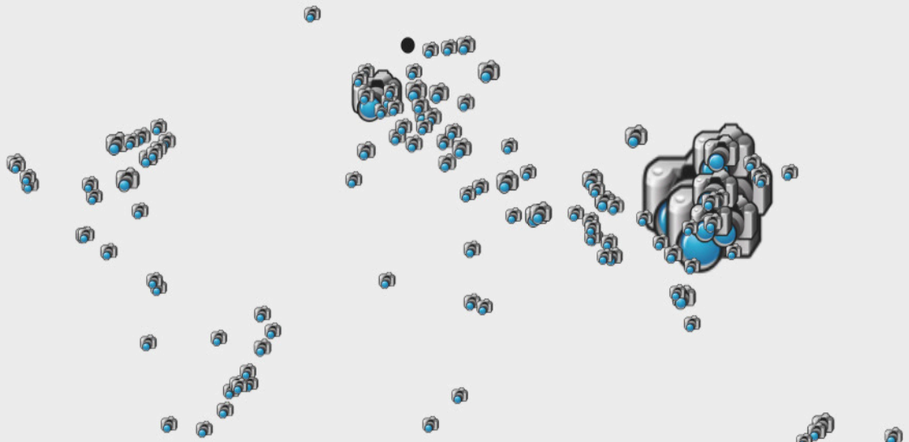
The law section consists of GDPR guidelines and rules regarding facial recognition system in United Kingdom, and all the rules concerning the technology. All the parts of GDPR are thoroughly covered in points.

Design development is the research part of the project, which explains and explores how different methods were used to form the outcome.

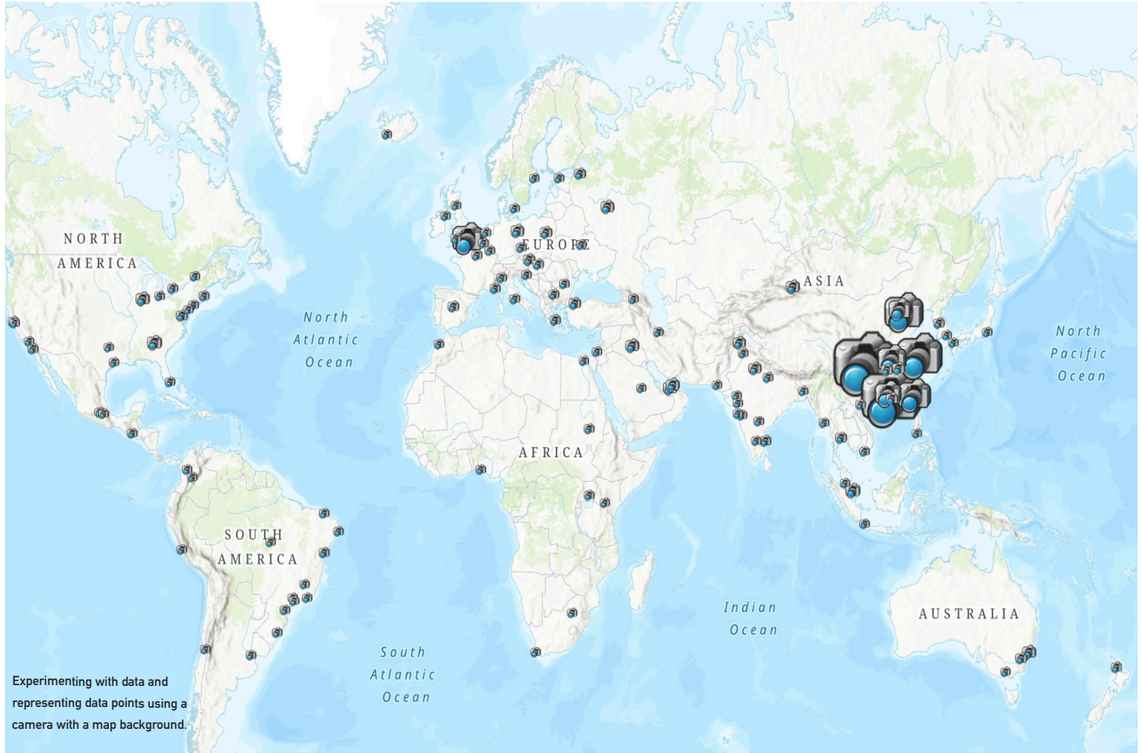
The project is a wholesome collection and guide to facial recognition, and it's concerns in the UK. Keeping in mind different approaches from various practitioners I believe facial recognition is a very good technology when used with rules and guidelines.

It's fast, convenient and secure, nonetheless there are concerns with privacy whilst using facial recognition and surveillance.

In a hypothetical perfect world, I believe there wouldn't be any surveillance and this project won't exist. But here we are, learning about facial recognition and surveillance.



Experimenting with data and representing data points using a camera without a background.



Experimenting with data and representing data points using a camera with a map background.

Bibliography

Webpage

Ada Lovelace Institute (2019) Beyond face value: public attitudes to facial recognition technology Available at https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf (Accessed: 10 October 2019).

Wong Dennis (2019) Big brother is watching you: the world's top 100 most surveilled cities Available at https://multimedia.scmp.com/infographics/news/world/article/3034080/most-surveilled-cities/index.html (Accessed: 23 October 2019)

Gladstone Nikki (2018) How Facial Recognition Technology Permeated Everyday Life Available at https://www.cigionline.org/articles/how-facial-recognition-technology-permeated-everyday-life (Accessed: 9 October, 2019.)

Navlakha Meera (2019) Eight Of The Ten Most-Surveilled Cities In The World Are In China Aviliable at https://www.vice.com/en_in/article/9keya8/most-surveilled-cities-in-the-world-china (Accessed: 27 October, 2019).

Thomas Elise (2019) How to hack your face to dodge the rise of facial recognition tech Available at https://www.wired.co.uk/article/avoid-facial-recognition-software (Accessed 13 October, 2019).

Ng Lance (2019) How to Beat Facial Recognition Available at https://medium.com/@lancengym/how-to-beat-facial-recognition-ab118a0c37fd (Accessed 15 October, 2019).

Gonzalez Robbie (2014) Computers Wrote the Caption for This Photograph, and Changed Everything Available at https://io9.gizmodo.com/computers-wrote-the-caption-for-this-photograph-and-ch-1660450610 (Accessed 10 October, 2019).

Sample Ian (2019) What is facial recognition - and how sinister is it? Available at https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it (Accessed 7 October, 2019).

Biometric data and data protection regulations GDPR and CCPA (2019) available at https://www.gemalto.com/govt/biometrics/biometric-data (Accessed October 15, 2019).

Information Commission Office (ico) (2018) Guide to the General Data Protection Regulation (GDPR) Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (Accessed 17 October 2019).

Gayle Damien (2019) Privacy campaigners warn of UK facial recognition 'epidemic' Available at https://www.theguardian.com/technology/2019/aug/16/privacy-campaigners-uk-facial-recognition-epidemic (Accessed 6 October 2019).

Bischoff Paul (2019) The world's most-surveilled cities Available at https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ (Accessed: 12 October 2019).

Police arrest passenger who boarded plane in Hong Kong as an old man in flat cap and arrived in Canada a young Asian refugee 2011 Available at https://www.dailymail.co.uk/news/article-1326885/Man-boards-plane-disguised-old-man-arrested-arrival-Canada.html (Accessed: 13 October 2019)

Elise Thomas (2019) How to hack your face to dodge the rise of facial recognition tech Available at https://www.wired.co.uk/article/avoid-facial-recognition-software (Accessed 13 October, 2019).

Big Brother Watch (2019) About us https://bigbrotherwatch.org.uk/about/who-we-are/ (Accessed: 14 October 2019)

Big Brother Watch (2018) Face-Off: The lawless growth of Facial recognition in UK policing Available at https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf (Accessed: 15 October 2019)

Yaroslav Kuflinski (2019) How Ethical Is Facial Recognition Technology? Available at https://towardsdatascience.com/how-ethical-is-facial-recognition-technology-8104db2cb81b (Accessed: 5 October 2019).

Millward James A (2018) What It's Like to Live in a Surveillance State Available at https://www.nytimes.com/2018/02/03/opinion/sunday/china-surveillance-state-uighurs.html (Accessed 5 November 2019).

Books

McCahill Mike (2002) The Surveillance Web New York by Routledge.

Publications

Field, T. M., Cohen, D., Garcia, R., & Greenberg, R. (1984). Mother-stranger face discrimination by the newborn. Infant Behavior and Development, 7(1), 19–25. Available at doi:10.1016/s0163-6383(84)80019-3 (Accessed 08 October, 2019).

You have zero privacy anyway. Get over it.

- Scott McNealy, Co-Founder Sun Microsystems