

Camera Obscura

Tom Isaacson

@parsley72

2020 Protests

- Black Lives Matter
- Hong Kong democracy
- Climate Change
- Anti-lockdown / Anti-vax / 5G / chemtrails / Lizard people

<https://www.cnet.com/news/police-use-of-social-media-is-under-a-microscope-amid-protests/>

2021 Protests (new content!)

- Storming of US Capitol

“Miami PD says it is using facial recognition tech from Clearview AI to identify Capitol rioters, raising concerns among civil liberty and privacy advocates”

<https://www.bloomberg.com/news/articles/2021-01-16/selfie-snapping-rioters-leave-fbi-a-trail-of-over-140-000-images>

Clearview.ai

Using public data from social media, providing facial recognition to law enforcement, ICE, Macy's, Walmart, and the NBA.



<https://malicious.life/episode/episode-103/>

PimEyes

<https://pimeyes.com/>

Face Search Engine Reverse Image Search

FACIAL RECOGNITION SEARCH TOOL. UPLOAD YOUR
PHOTO AND FIND WHERE IMAGES WITH YOUR FACE
APPEAR ONLINE.

Have your photos been used?

<https://exposing.ai/>

| DATASET | FLICKR PHOTOS* | PURPOSES** |
|-----------|----------------|------------------|
| DiveFace | 115,729 | Face recognition |
| FaceScrub | 211 | Face recognition |
| IJB-C | 5,757 | Face recognition |
| MegaFace | 3,581,071 | Face recognition |
| PIPA | 32,518 | Face recognition |
| VGG Face | 13,955 | Face recognition |

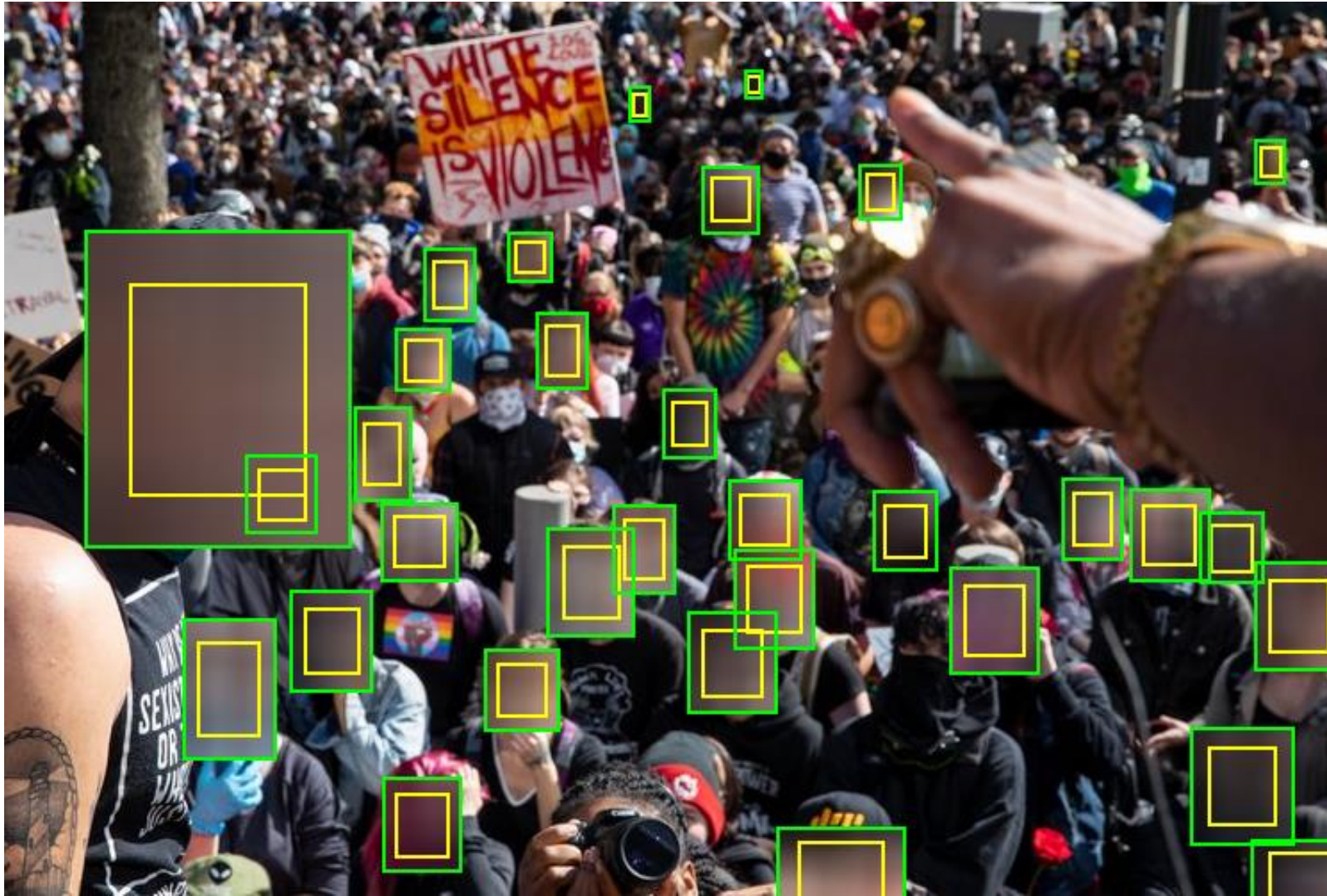
Signal app

<https://signal.org/blog/blur-tools/>



Vframe.io

<https://github.com/vframeio/vframe> faceless plugin



Fawkes

<http://sandlab.cs.uchicago.edu/fawkes/>

Original



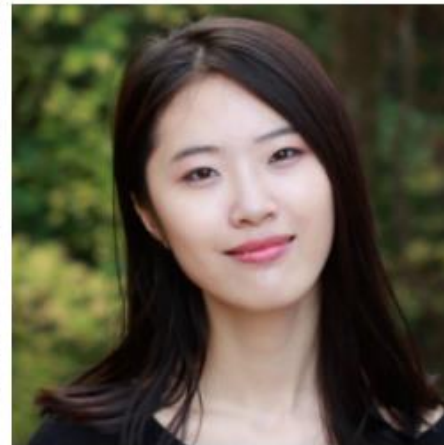
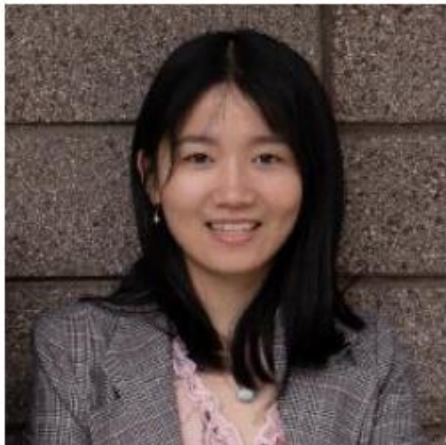
Cloaked



Original



Cloaked



Ben Loula “Easy Anti-Rekognition Techniques”

ChCon 2020 talk: https://2020.chcon.nz/talks/ben_l/

“Is there a way to easily avoid getting picked out of a crowd by facial recognition software, preferably without running afoul of anti-mask laws? Let’s fire up Amazon Rekognition and find out!”

Slides:

https://docs.google.com/presentation/d/1OlgwdtDq6hSMe27PJoLUota_g0dAJXlHH74AQyUszAYA/edit?usp=sharing

Fawkes test on AWS Rekognition #1

Reference face



Comparison faces



[Read feature documentation to learn more](#)
Issues or questions? Use feedback button on bottom-left.

▼ Results



Similarity 99.9 %

► Request

► Response

Fawkes test on AWS Rekognition #2

Reference face



Comparison faces



[Read feature documentation to learn more](#)
Issues or questions? Use feedback button on bottom-left.

▼ Results

 $=$ 

Similarity 99.9 %

► Request

► Response

Uni. of Maryland's Invisibility Cloak project











<https://www.cs.umd.edu/~tomg/projects/invisible/>





CCTV around the world

<https://www.precisecurity.com/articles/Top-10-Countries-by-Number-of-CCTV-Cameras>

| | Country | # of CCTV Cameras | # of People | # of CCTV Cameras per 100 People |
|---|----------------|-------------------|---------------|----------------------------------|
|  | United States | 50 000 000 | 327,167,430 | 15.28 |
|  | China | 200 000 000 | 1,392,730,000 | 14.36 |
|  | United Kingdom | 5 000 000 | 66,488,990 | 7.5 |
|  | Germany | 5 200 000 | 82,927,920 | 6.27 |
|  | Netherlands | 1 000 000 | 17,231,020 | 5.80 |
|  | Australia | 1 000 000 | 24,992,370 | 4 |
|  | Japan | 5 000 000 | 126,529,100 | 3.95 |
|  | Vietnam | 2 600 000 | 95,540,400 | 2.72 |
|  | France | 1 650 000 | 66,987,240 | 2.46 |
|  | South Korea | 1 030 000 | 51,635,260 | 1.99 |

Facial Recognition World Map

<https://surfshark.com/facial-recognition-map>





UNITED STATES

More than **50% of all Americans** are currently in police facial recognition databases.



BELGIUM

Belgium is so far the only country to find facial recognition in breach of national law.



TURKEY

The Turkish military recently purchased **30 kamikaze drones** with facial recognition capabilities.



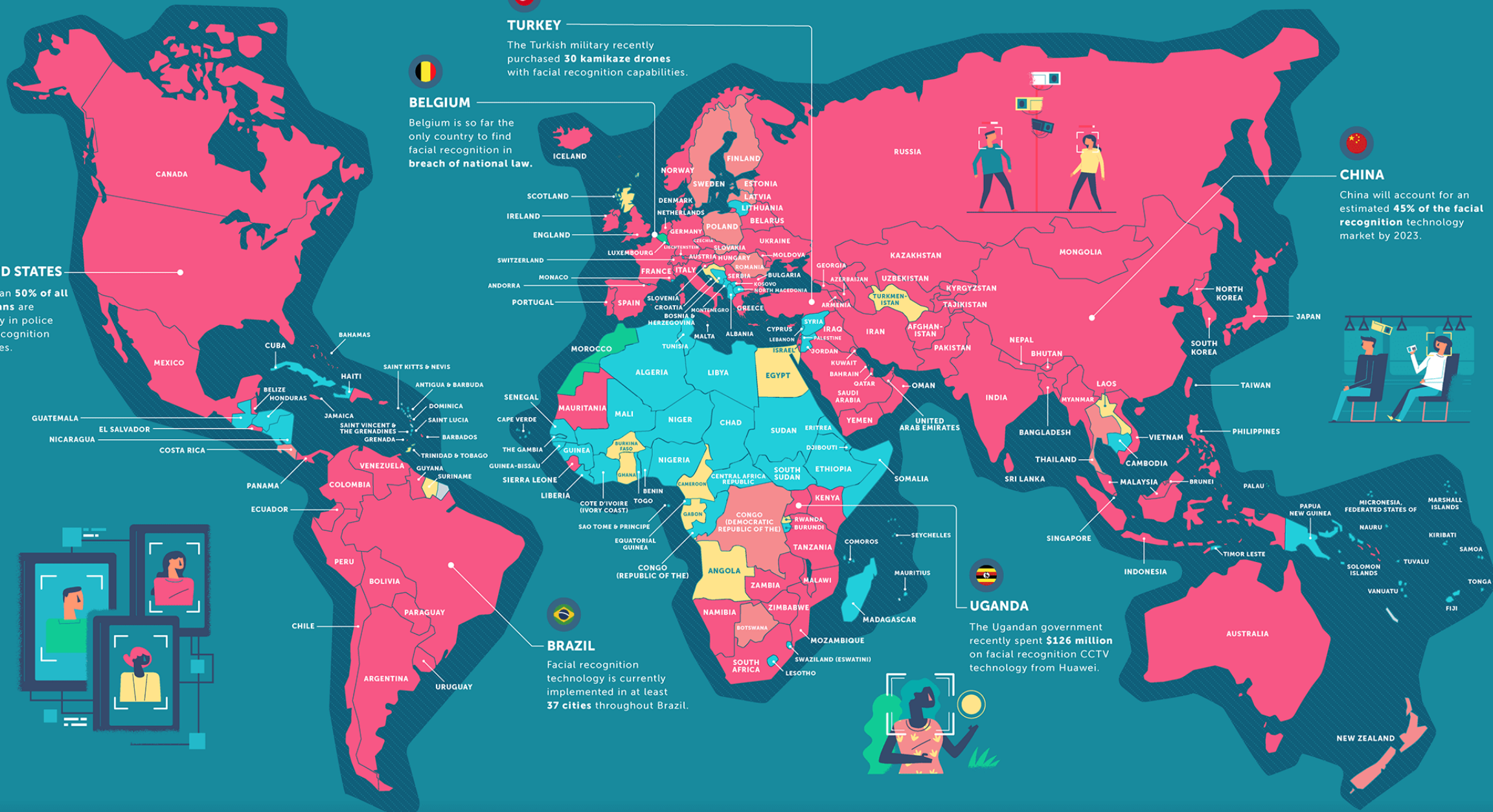
CHINA

China will account for an estimated **45% of the facial recognition** technology market by 2023.



UGANDA

The Ugandan government recently spent **\$126 million** on facial recognition CCTV technology from Huawei.



Bans on facial recognition

San Francisco: <https://www.theverge.com/2019/5/14/18623013/san-francisco-facial-recognition-ban-vote-city-agencies>

Boston: <https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban>

Oakland: <https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php>

Portland: <https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology>

NZ Police

31 August 2020: Police setting up \$9m facial recognition system which can identify people from CCTV feed

<https://www.rnz.co.nz/news/national/424845/police-setting-up-9m-facial-recognition-system-which-can-identify-people-from-cctv-feed>

“Both [NZ Police and Internal Affairs Department] said they did not tell the public as these are mere upgrades.”

Privacy By Design

Ann Cavoukian (former Information and Privacy Commissioner for Ontario, Canada) published in 2010:

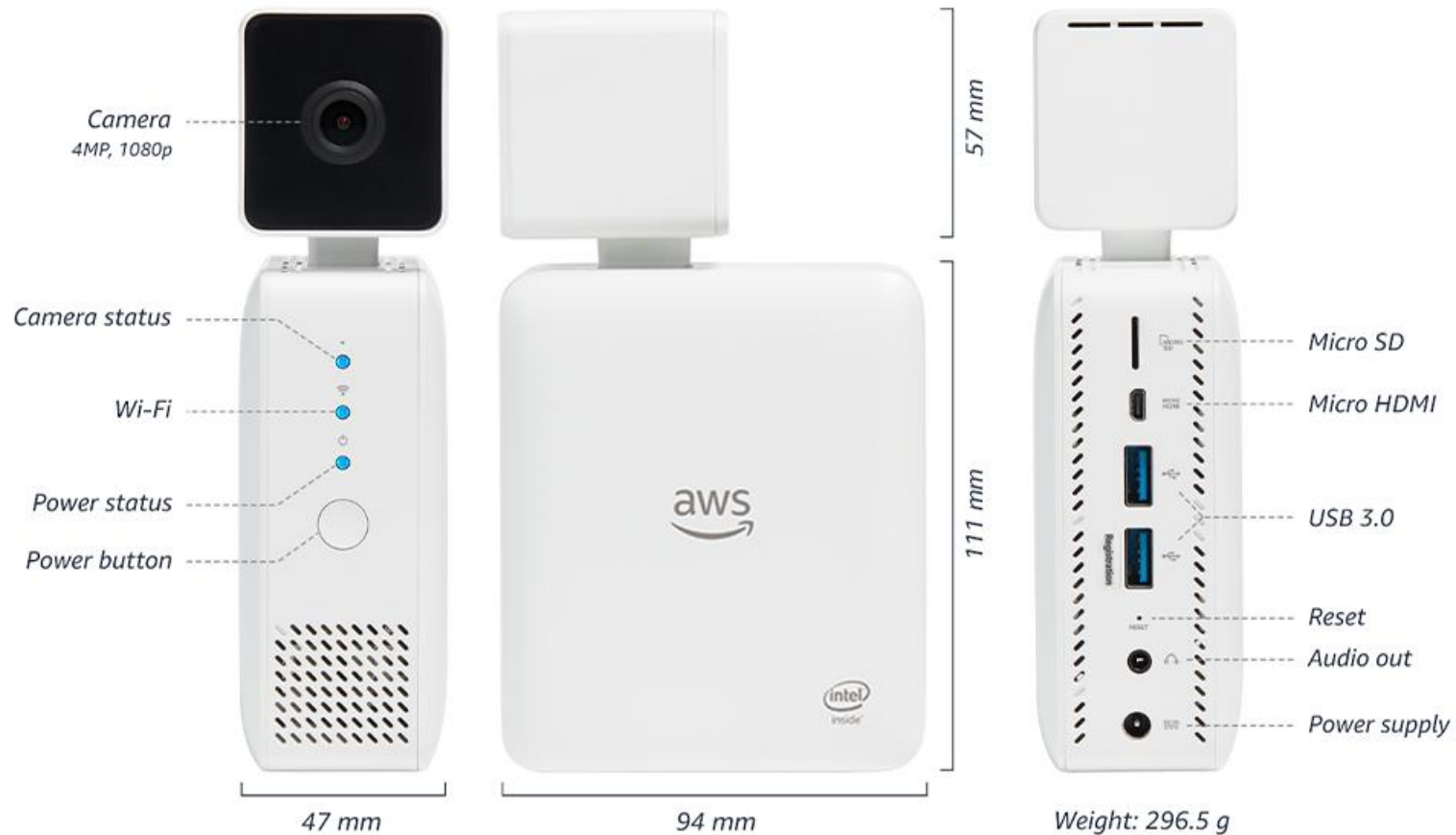
1. Proactive not Reactive; Preventative not Remedial.
2. Privacy as the Default.
3. Privacy Embedded into Design.
4. Full Functionality - Positive-Sum, not Zero-Sum.
5. End-to-End Security - Lifecycle Protection.
6. Visibility and Transparency.
7. Respect for User Privacy.

Machine Learning (ML) Cameras at the Edge

- NVidia Jetson – “Autonomous Machine”
- Intel Myriad – “VPU with Neural Compute Engine”
- Ambarella - “AI Vision Processors For Edge Applications”

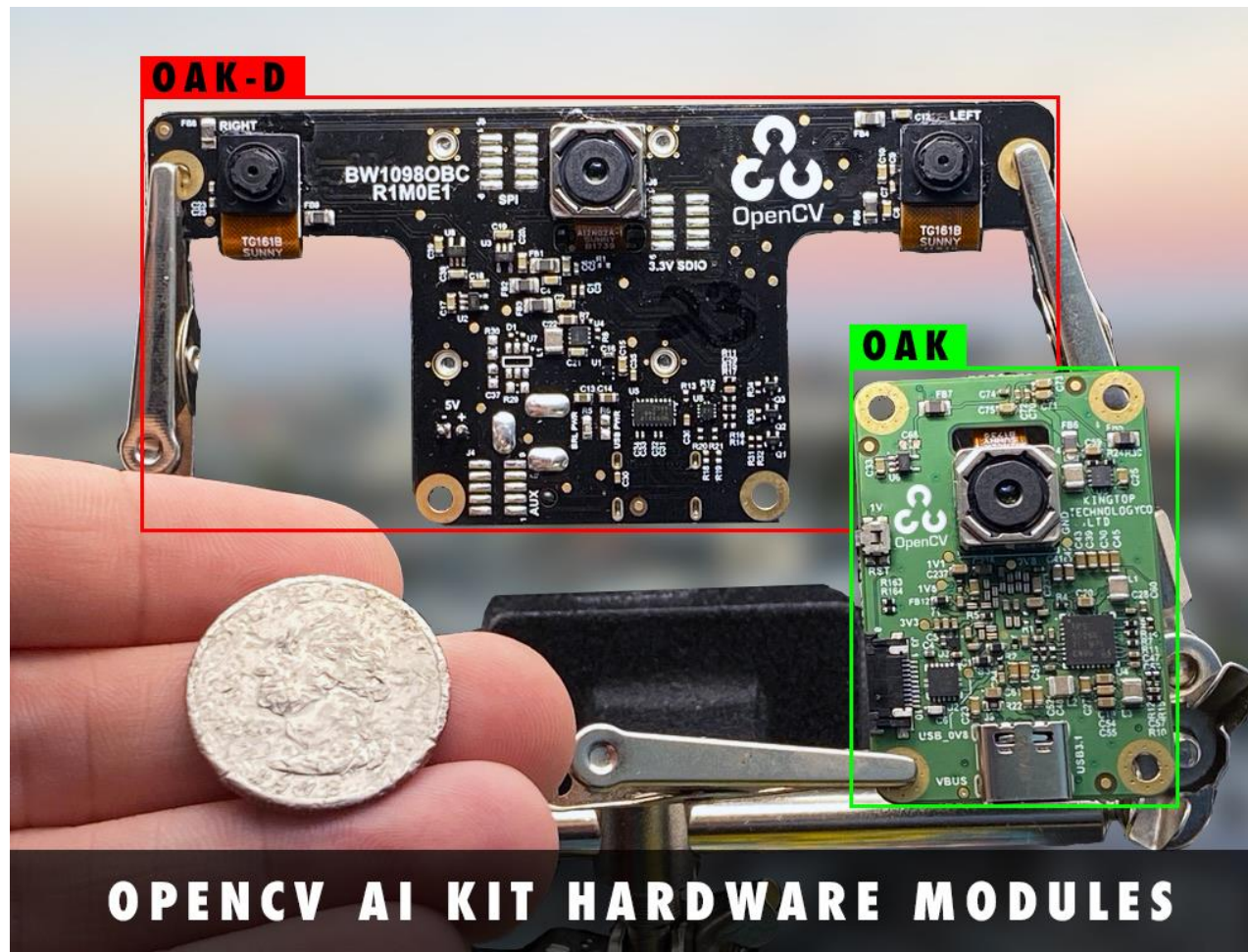
AWS DeepLens

<https://aws.amazon.com/deeplens/>



OAK: Spatial AI Powered by OpenCV

<https://opencv.org/introducing-oak-spatial-ai-powered-by-opencv/>

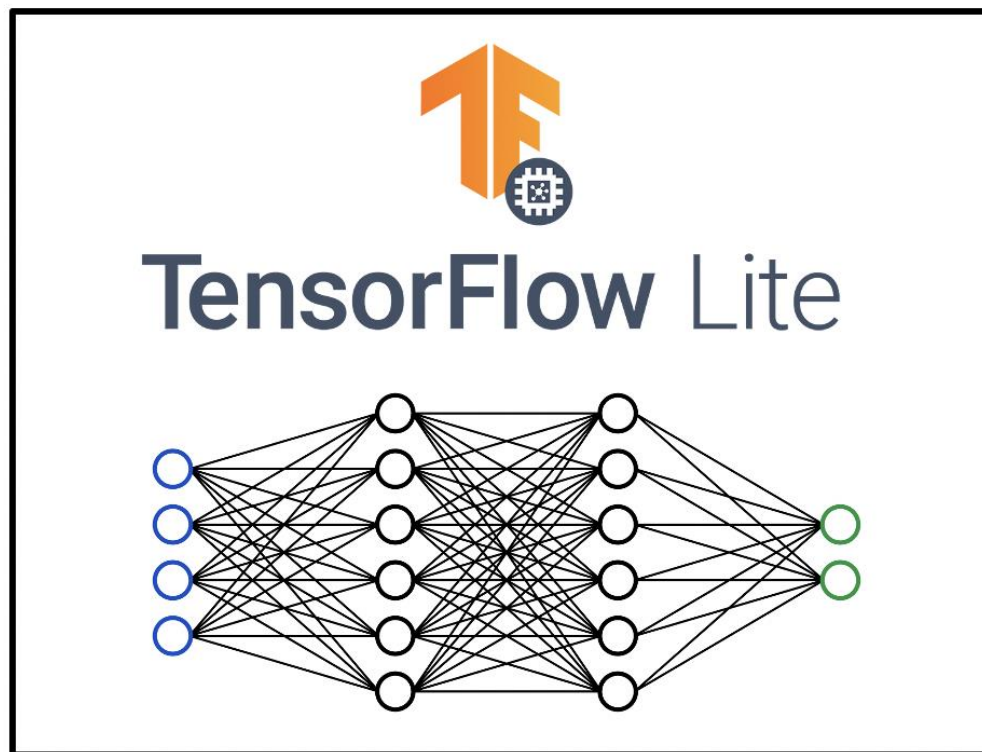


“Vizy” AI Camera

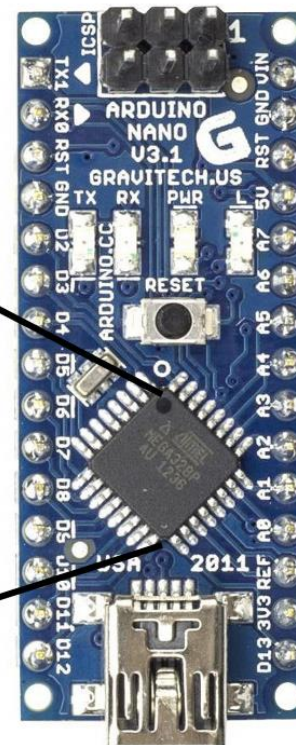
<http://linuxgizmos.com/12mp-raspberry-pi-based-ai-camera-supports-300fps-video/>



TinyML



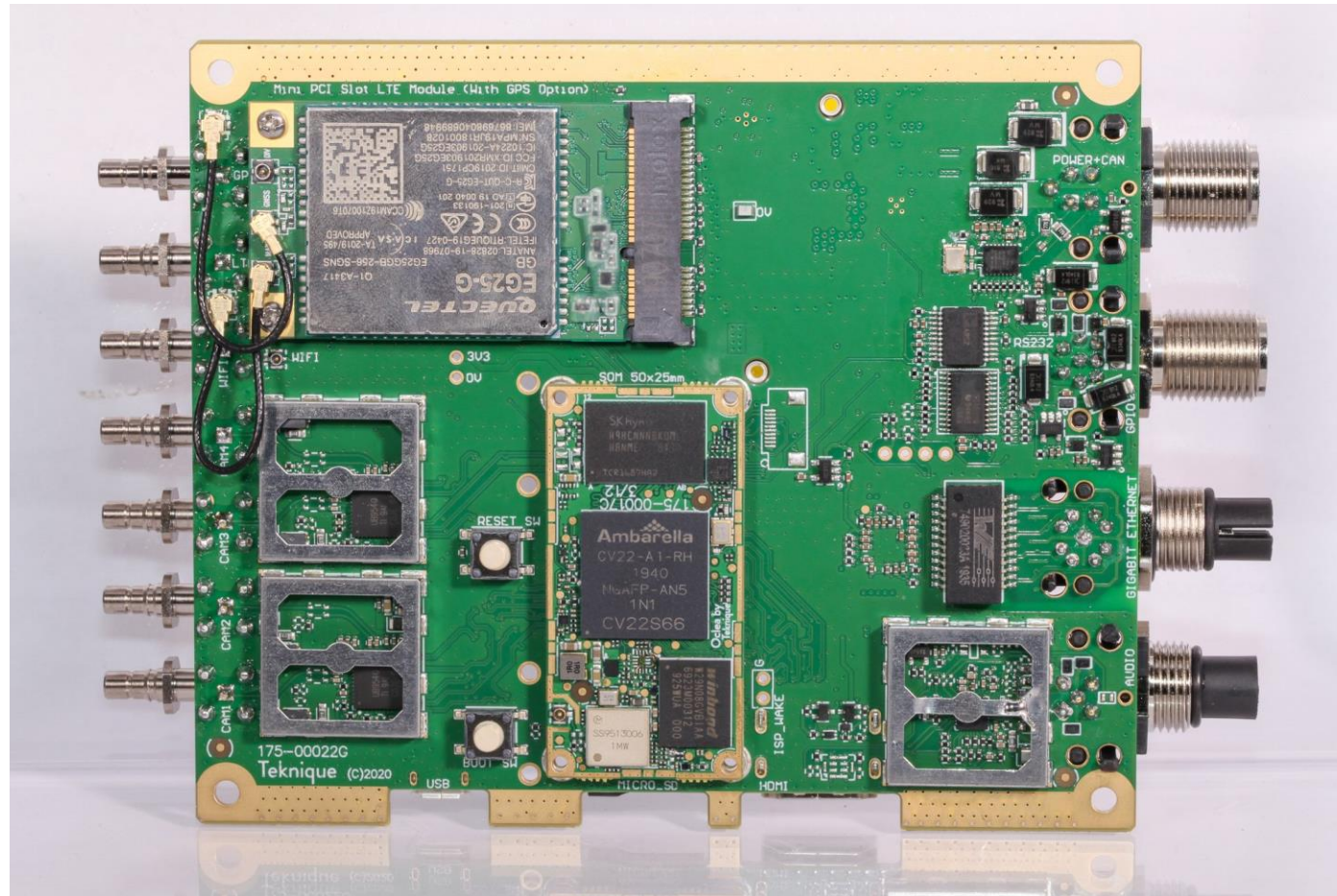
- [1] Training
- [2] Distillation
- [3] Quantization
- [4] Encoding
- [5] Compilation



TinyML

Teknique

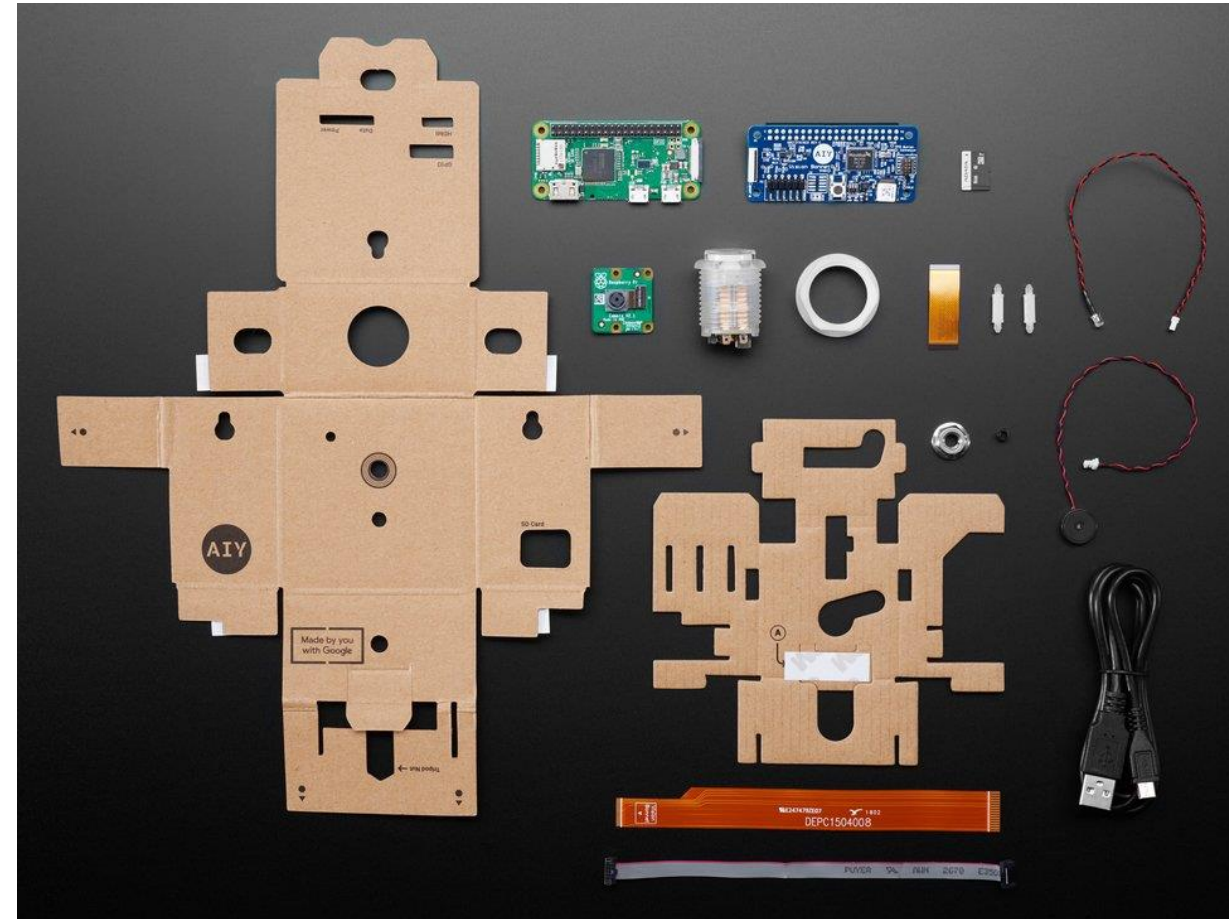
Oclea <https://store.oclea.com/>



Demo time

Google DIY AI Vision Kit

<https://aiyprojects.withgoogle.com/>



CCTV for Pedestrian Traffic Analysis



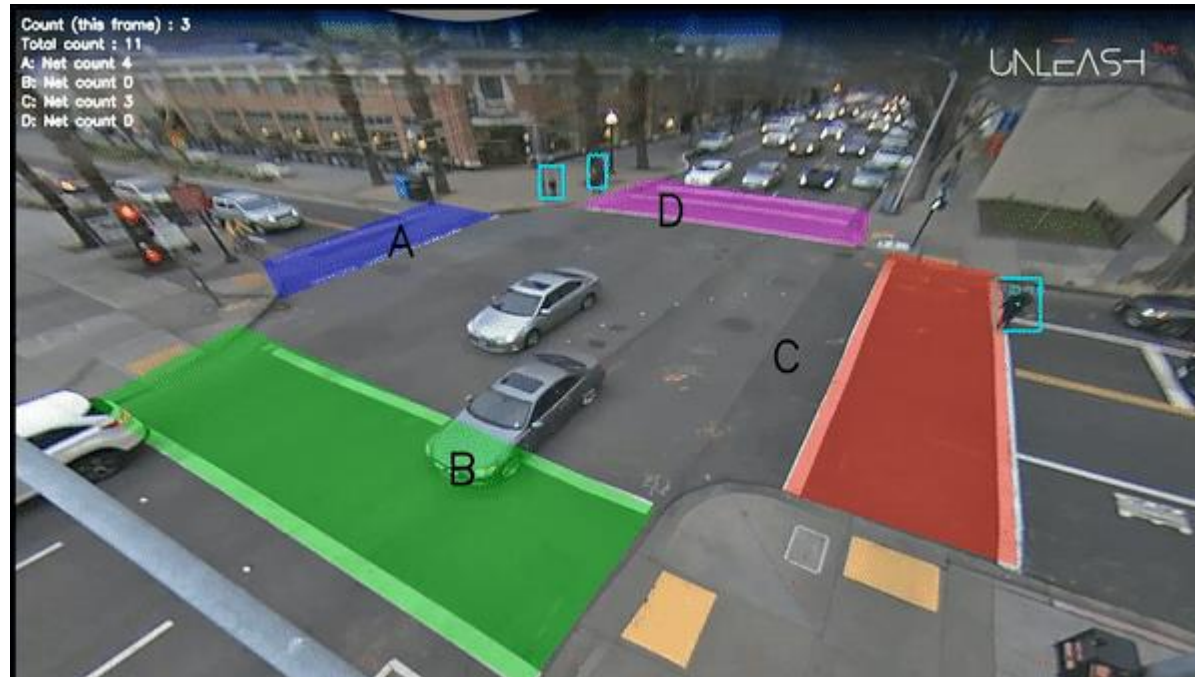
Facial recognition on the camera

Push the description of the face (128 dimension vector) to the camera.



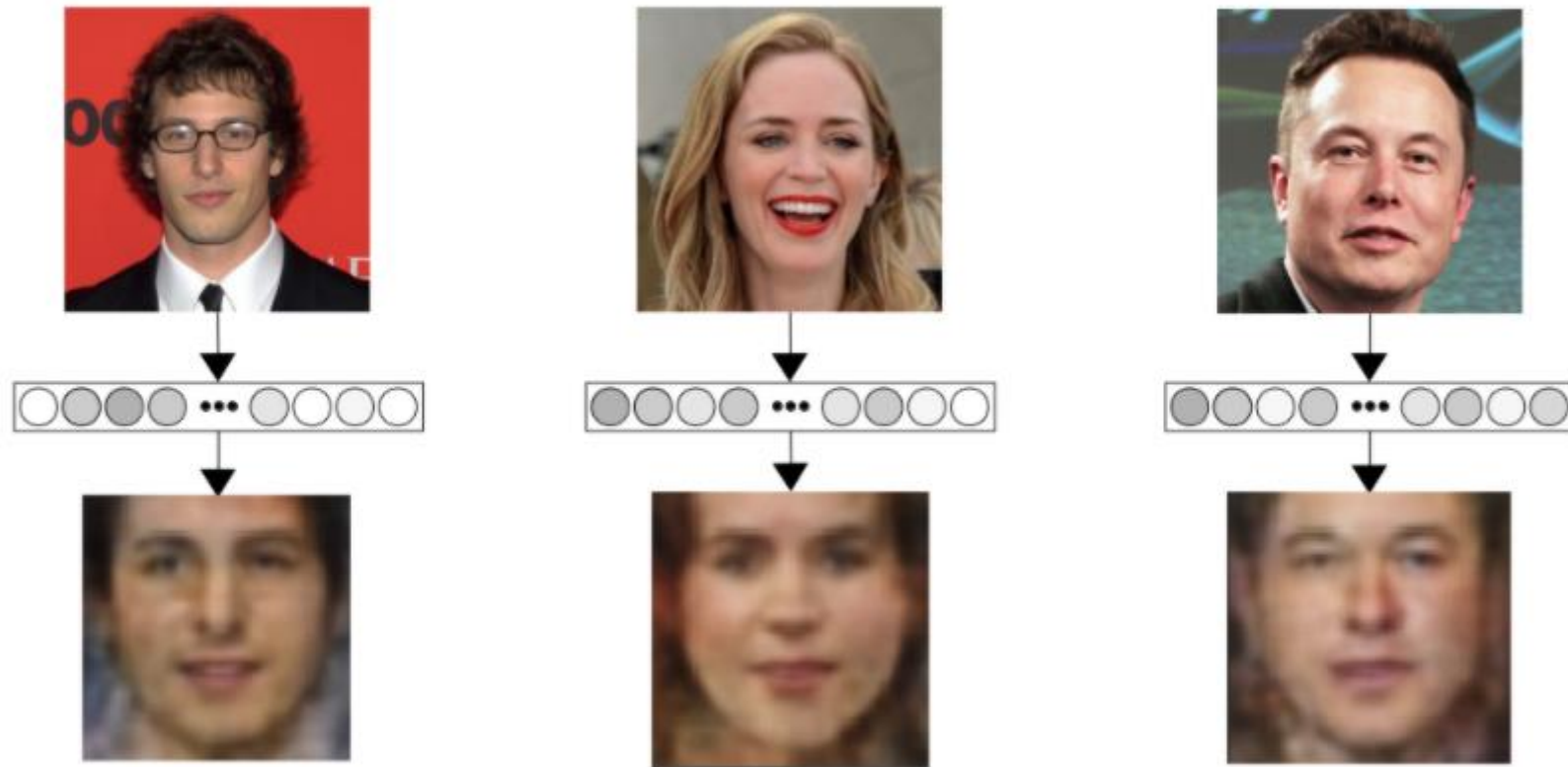
CCTV with multiple cameras

Share description of face.

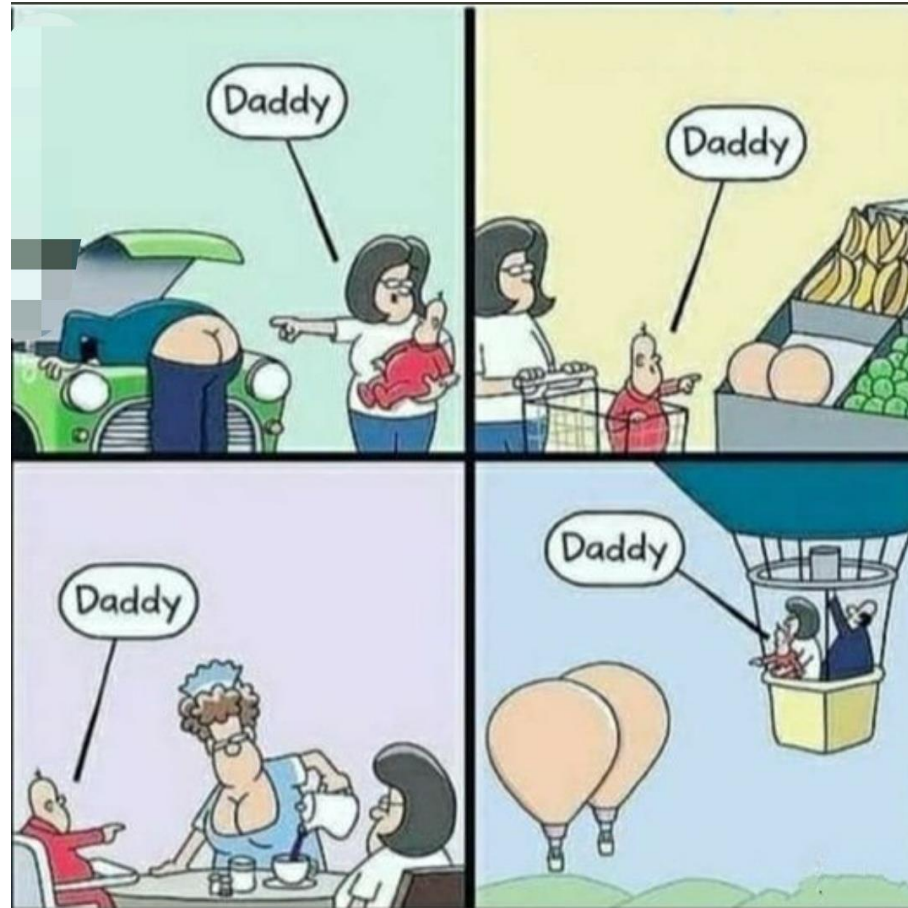


Inverting Facial Recognition Models

<https://blog.floydhub.com/inverting-facial-recognition-models/>



Issues with facial recognition



Types of facial recognition

Facial recognition:

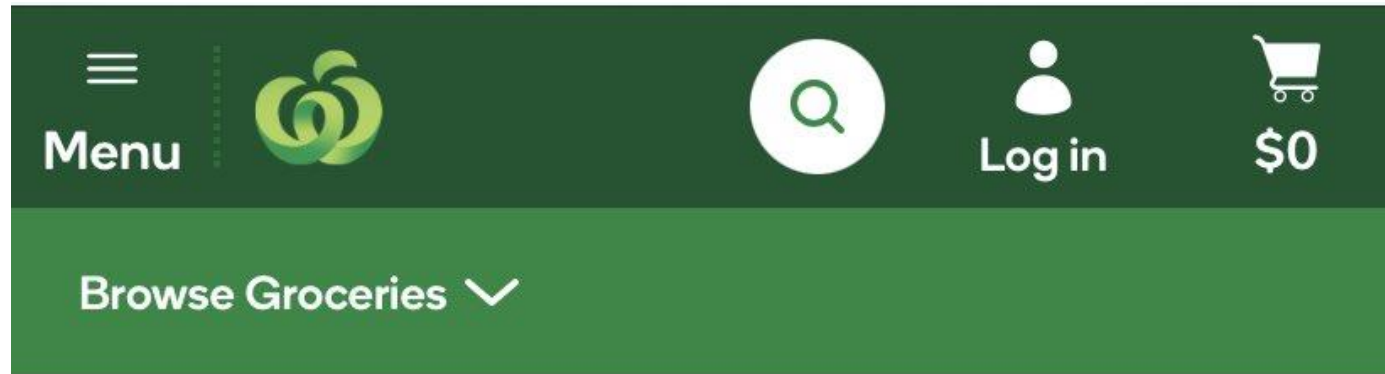
- Looking up faces on a database to identify them

Person tracking / tagging:

- Remembering individual faces/ears/clothing/gait without identifying them

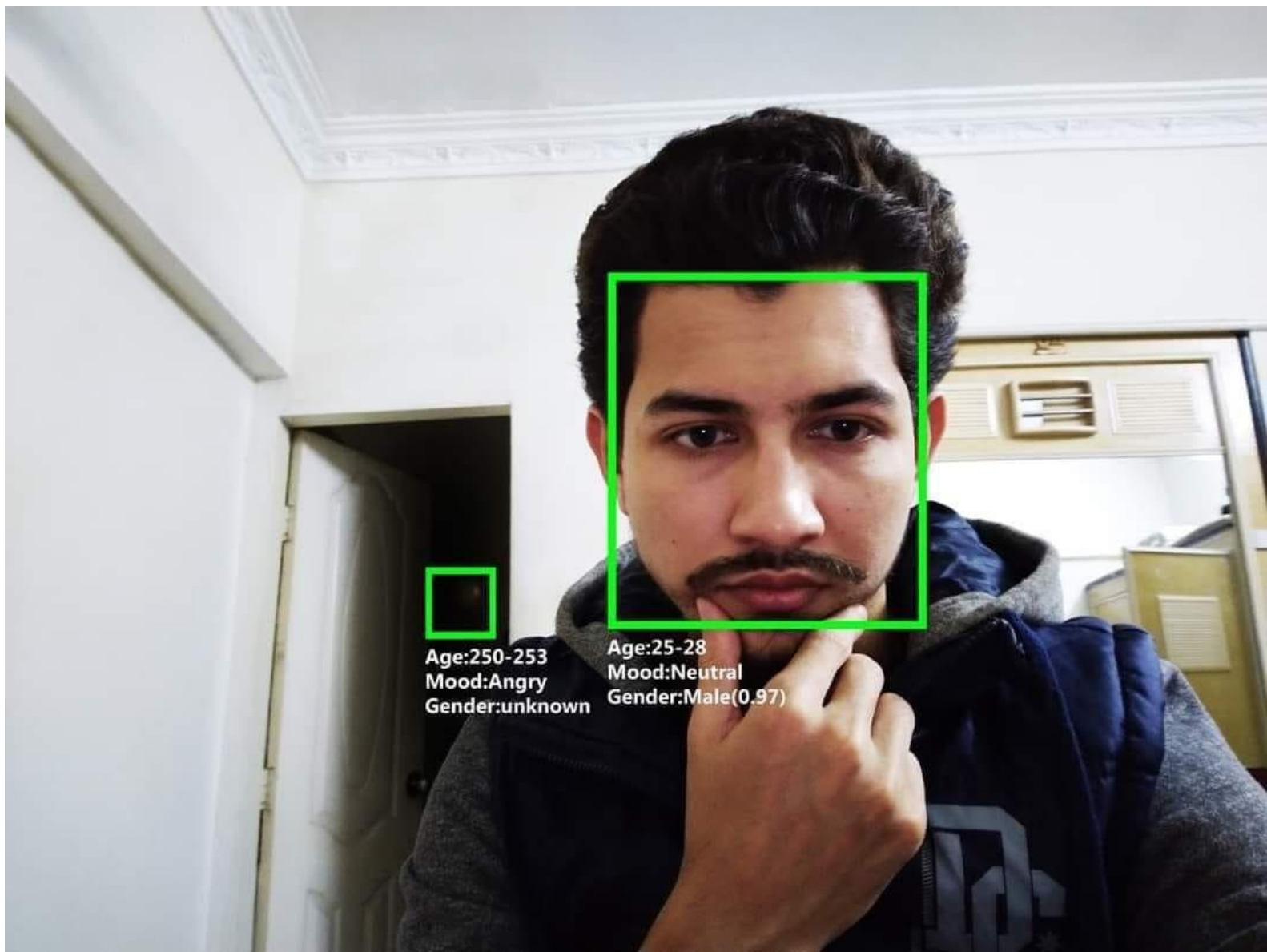
UK: Co-op facial recognition trial raises privacy concerns

<https://www.bbc.com/news/technology-55259179>



When you visit us in person, including for events:

- your contact details and loyalty card number for in-store services such as pick up, home delivery or special orders
- we may ask for your ID, such as your driver's licence, if you purchase alcohol or tobacco
- cameras (including security and smart cameras) may record footage and other data which may identify you



Age:250-253
Mood:Angry
Gender:unknown

Age:25-28
Mood:Neutral
Gender:Male(0.97)

Tracking in shops

- Age/gender/emotion
- How they move around the shop
- List of previous offenders

Home / door cameras

ADT Tech Hacks Home-Security Cameras to Spy on Women

<https://threatpost.com/adt-hacks-home-security-cameras/163271/>

Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs

<https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats>

Ring adds end-to-end encryption to protect your video streams

<https://www.theverge.com/2021/1/13/22225716/ring-end-to-end-encryption-video-launch>

Ring doorbells to send live video to Mississippi police

<https://www.bbc.com/news/technology-54809228>

US Police/Fire participation in Amazon Ring/Neighbours by Ring

<https://www.google.com/maps/d/viewer?mid=1eYVDPH5itXq5acDT9b0BVeQwmESBa4cB>





Cybergibbons

@cybergibbons

Normal 0%



Given that the NurseryCam issues concern video data of kids, I am shortcutting normal disclosure.

This is my choice.

The system they have implemented is fundamentally insecure and has been for years.

I am disgusted by their attitude to security, over a long period.

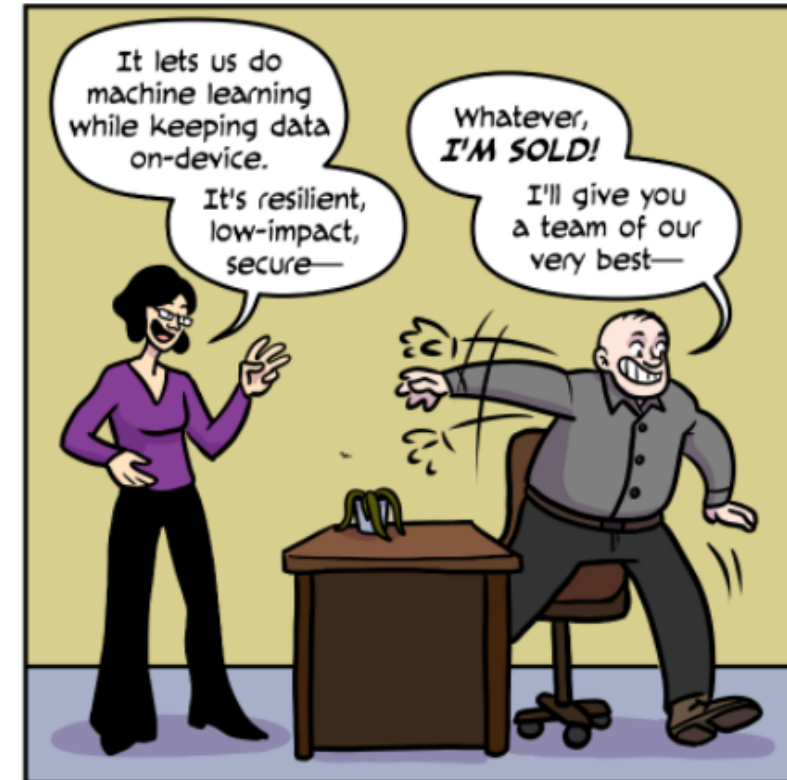
9:03 AM · Feb 13, 2021 · Twitter Web App

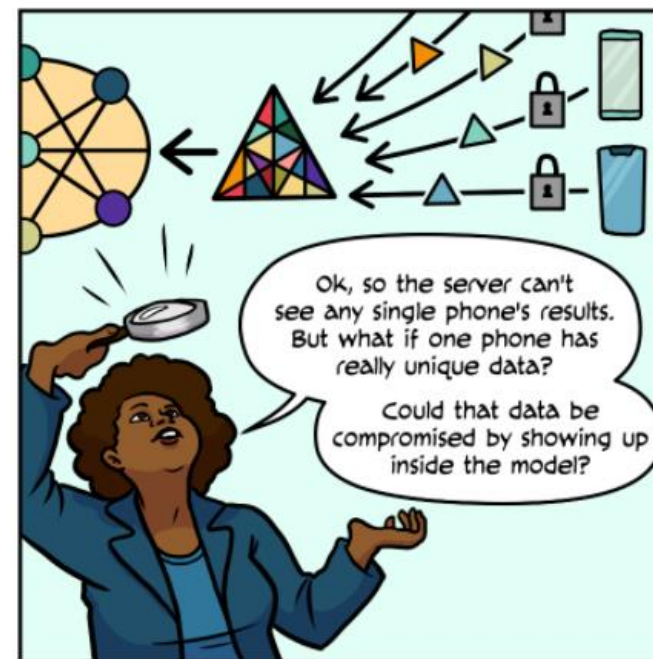
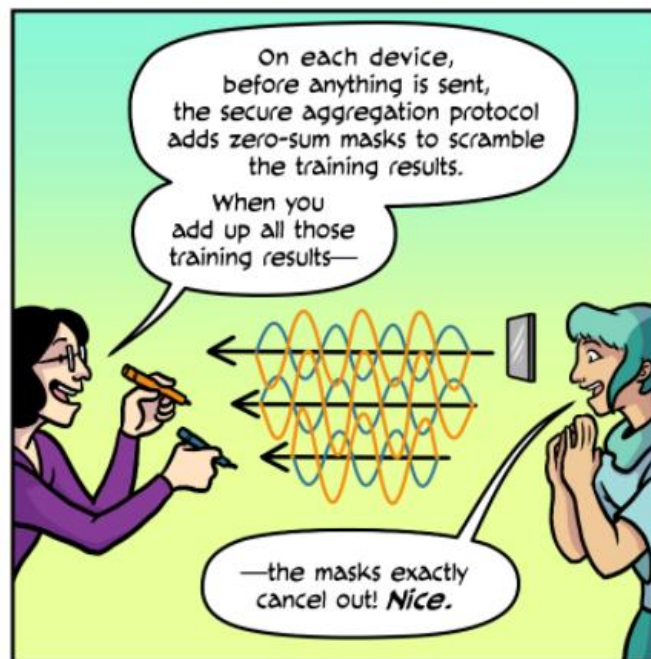
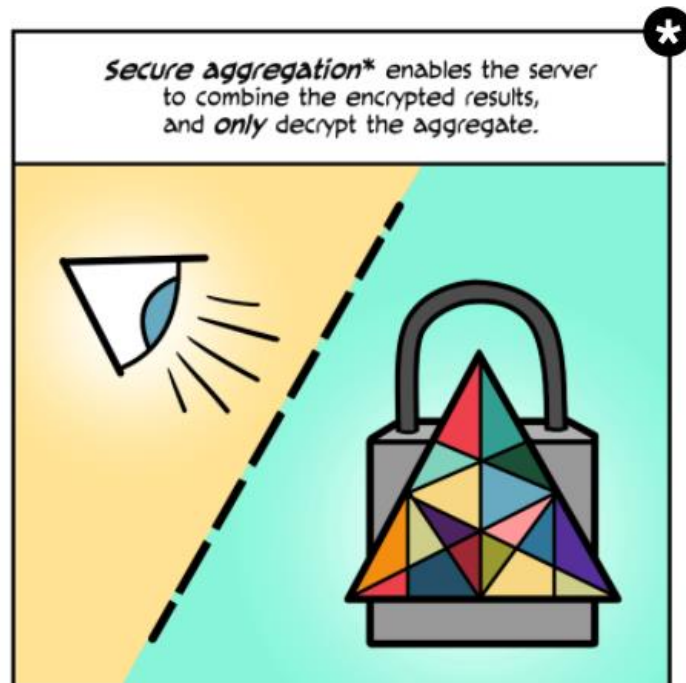
What features should a door camera have?

- Movement/person detection
- Recognition of residents / family members / friends
- Package detection (addition and removal)
- Mic/speaker for answering door when you're not there
- Remote login

Federated Learning

<https://federated.withgoogle.com/>





Tuesday Feb 23rd, Wellington [@CivilLibertyNZ](https://twitter.com/CivilLibertyNZ)



The New Zealand Council for Civil Liberties presents

Facial Recognition and Human Rights

| | |
|-------------------|--|
| Dr Marcin Betkier | - Law-professor, Co-author of the Law Foundation report Facial Recognition Technology in NZ |
| Dr Andrew Chen | - Research fellow at Koi Tū : The Centre for Informed Futures |
| Karaitiana Taiuru | - Academic, author of Māori Cultural Considerations with Facial Recognition Technology |
| Lisa Woods | - Campaign director at Amnesty International |

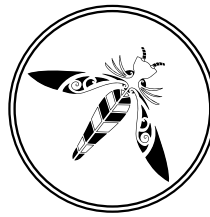
6pm, Southern Cross Bar, Wellington, free entry, doors from 5:30pm, R18

“The Computers Have a Thousand Eyes: Towards a Practical and Ethical Video Analytics System for Person Tracking” (2019, Andrew Chen)

<https://www.andrewchen.nz/>

- Access: Who has access to the video feed or footage, including secondary data derived from the cameras?
- Human Influence: Is there a person-in-the-loop?
- Anonymity: Are the observed people in the footage personally identifiable or anonymous?
- Data Use: How will the data be used?
- Trust: Do we trust the owner of the surveillance camera network?

Thank You to Our Sponsors and Hosts!



OWASP
**NEW
ZEALAND**
owasp.org.nz



DATACOM



myob



VOCUS



Without them, this Conference couldn't happen