

RESEARCH

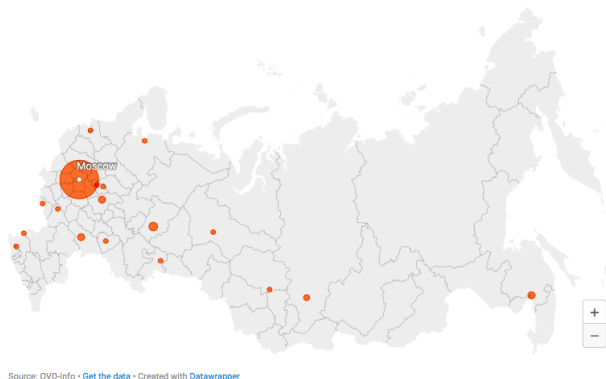
<https://reports.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters#3>

“We believe that the increase in **the number of post factum detentions is based on the development of technologies for monitoring social networks and facial recognition**: authors of posts with information about the events are equated with the organizers, and **people identified by video recordings are declared participants**.”

“In May 2017, the official website of the Mayor of Moscow [reported](#) that more than **3.5 thousand cameras** have been connected to the Unified Data Storage and Processing Center (ECHD), including more than 1.6 thousand at the entrances to residential buildings. And already in September, **more than three thousand city surveillance cameras were connected to the facial recognition system**.”

“Although the mass wearing of medical masks during the pandemic could become an obstacle to facial recognition, the developer of biometric recognition Anton Maltsev believes that this problem may have already been solved: ... examining the case files of those held liable «post factum», OVD-Info found at least one case in Moscow **when a person was detained on the basis of a photo and video, although in both images he was wearing a medical mask**.”

“Although this was most often reported by residents of Moscow, this practice is not limited to the capital: similar evidence was received from at least 17 other cities.” ->>>>



“Since at least [2012](#), **participants of the protest events have been illegally photographed at police stations**. This practice has managed to take root and has become widespread. ...

Illegal photographing of detainees is one of the most common violations occurring at police stations.”

“Alexey Shlyapuzhnikov, an expert on security and identification technologies at Transparency International, [notes](#) that such photos can be used for recognition:

«The system includes the modules „Sherlock“ — search through the passport database — and PSKOV, which also works with social networks ... **the more photos of a person in this system, the easier it is to find them** — a photo for a national ID or a passport, in a criminal case, or a person was detained and taken to a police station. Therefore, everyone is being photographed intensively during detentions. The more high-quality photos from different angles posted on a social network, the easier it is for the system to recognize a person.”

“Initiation of a case

If a person who visited a protest event is captured by a video surveillance camera, an administrative case may be opened against them already after the event. According to the experts we interviewed, this probability increases if a participant of the event looked directly into the camera — in this case, it is easier for the algorithm to recognize the face.”

“People identified by cameras after the protest of April 21 most often reported police visits to the official residence address, although sometimes officers also established the actual living address.”

“By itself, the collection of data on the participants of the protests by the state creates the risk of politically motivated persecution.”

<https://www.eff.org/document/transcript-observing-police-surveillance-protests-november-2020>

How to spot police surveillance technologies while attending protests

Police surveillance tech is



On police officers' bodies



On vehicles and roadways



In the air



In the environment

Body-Worn Cameras

Learn whether local law enforcement uses body-worn cameras and the potential brand at atlasofsurveillance.org/search.

APPEARANCE: Varies by model.

DATA COLLECTED:

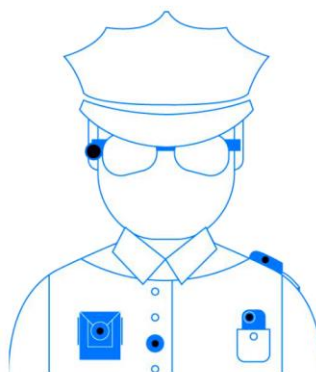
Surveillance of police brutality;
Surveillance of protesters.

FUNCTION:

Video cameras attached to uniforms. Each model functions differently.

HOW USED BY THE POLICE:

Varies by jurisdiction.
Some locations (e.g. Seattle) have a ban on police using BWCs at protests.



Mobile Biometric Devices

APPEARANCE: Handheld scanner; Can be a distinct device, or a phone/tablet using an app. Can look like police taking a photo.

DATA COLLECTED:

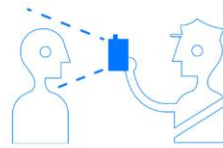
Biometric data (e.g. fingerprints, faces, irises, tattoos).

FUNCTION:

Compares data against existing biometric databases to identify people.

HOW USED BY THE POLICE:

Often used during detention, arrests, and checkpoints. It may be helpful to document incidents when police use cell phones to take photos.



**COP SCANNING
SOMEONE'S FACE**



**COP SCANNING
FINGERPRINT**

Automated License Plate Readers (ALPRs)

APPEARANCE: Camera pointed toward roads and traffic. Can be on trailers, surveillance towers, police vehicles, poles.

DATA COLLECTED:

Vehicle surveillance: License plates, make, color, bumper sticker text.

FUNCTION: ALPR data is uploaded to a central server that police can search. Police can also add vehicles to a watch list and receive alerts when a camera spots a vehicle.

HOW USED BY THE POLICE:

ALPR are often placed at fixed locations, such as streetlights and toll crossings, however mobile and semi-mobile ALPRs are more common with public gatherings.



Source: Mike Katz-Lacabe, CC-BY



Aerial Surveillance

APPEARANCE: Planes, helicopters, drones.

FUNCTION: Surveil protests from above.
May also use these aerial vehicles to communicate with crowds.

HOW USED BY THE POLICE:
May be equipped with high-definition cameras capable of either extreme wide-angle or extreme zoom videography. Also often equipped with thermal imaging.

This is a less common occurrence: aircraft may include ALPR, face recognition, video analytics, and cell-site simulators. These technologies would not be visible to observers.



Camera Networks

Depending on the neighborhood, it can be overwhelming to document every camera. Many cities are:

- installing networked surveillance cameras
- partnering with businesses to build camera networks

APPEARANCE: Varies.

DATA COLLECTED: High definition video, thermal imaging, object and pattern analysis.

FUNCTION: Can be held by citizens privately, owned by businesses, or connected to law enforcement.

HOW USED BY THE POLICE:
Varies.



[How Police Track Protesters With High-Tech Surveillance Tools](#)



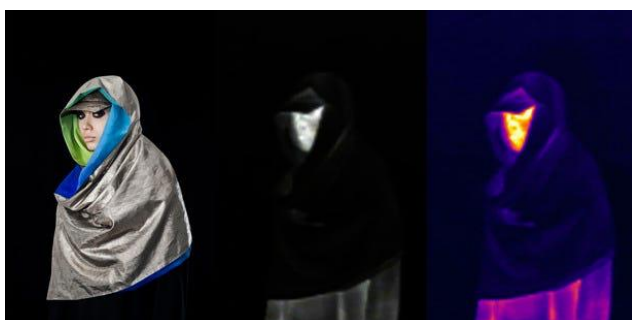
This video also tells something about **tattoo-recognition, iris-recognition and gunshot detection.**

How to distract facial recognition:

<https://www.popularmechanics.com/technology/security/g28719483/trick-surveillance-systems/?slide=1>



Hackers designed this skirt, which is covered in license plates with parts of the Fourth Amendment (the one that deals with unreasonable searches and seizures), to trip up surveillance systems. You can snag similarly designed hoodies, T-shirts, and tanks at [Adversarial Fashion's online store](#).



Anti-Surveillance Hijabs

Since 2009, artist Adam Harvey has been working on ways to create counter-surveillance fashion, which he calls [Stealth Wear](#).

One of his concepts (now sold out) is a scarf that you can wear like a hijab to disguise yourself from overhead drones.

Harvey makes his garments with silver-plated fabrics that can reflect thermal radiation. He believes that by 2050, countries will be able to perform full surveillance on their population for just .01% of GDP.

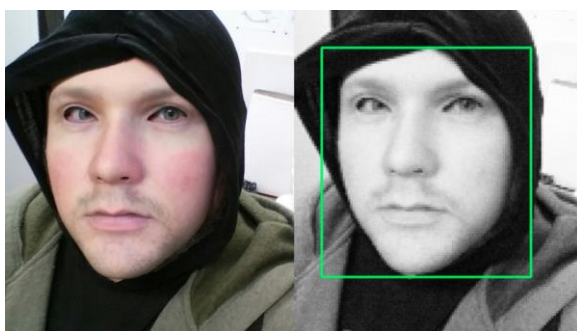


Fashionable Camouflage

Harvey is also the brains behind CV Dazzle, a project that looks at how fashion can be used as a form of camouflage against facial recognition tech.

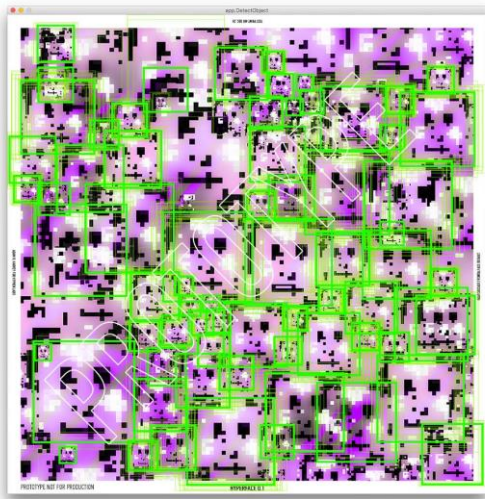
Try It:

1. **Create asymmetry.**
2. **Use tonal inverse.**
3. **Cover your nose bridge.**

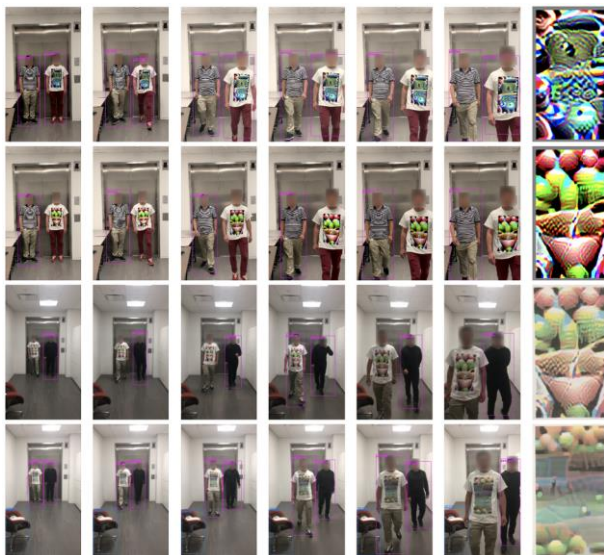


Using Someone Else's Face

[URME Surveillance](#) is a company dedicated to shielding people from facial recognition technology. The idea: get as many people as possible to wear a photo-realistic, 3D-printed prosthetic "face" resembling URME founder Leo Savaggio.



abstract patterns printed on shirts, which actually look like a face to facial recognition and algorithms.



T-shirts to Avoid People Detectors

New [research](#) put out in November 2019 by Northeastern University, in conjunction with the Massachusetts Institute of Technology's IBM Watson Lab in Boston, proposes a new type of T-shirt that allows people to mask themselves from people-detecting surveillance detectors by wearing tops with "adversarial" printed images on them.

<https://thehmm.nl/can-ar-filters-protect-us-against-facial-recognition-technology/>

Founders Gil Perry, Sella Blondheim and Eliran Kuta are [concerned about the integration of facial recognition systems](#) in public life and what governments will do with this data. That's why **they developed a tool that allows you to turn a photo of yourself into an AI-generated image of a person who doesn't exist but looks exactly like you to the human eye. In this way, the facial recognition technology cannot link the photo of your face to you as an individual person and your other data points online. Not only can the tool protect the privacy of citizens, it can also be used by privacy-sensitive organisations who hold large repositories of photos from employees or patients and need to comply with privacy regulations.** So far, this software is not yet available for personal use, but D-ID

looks into the possibility to do so in the future. D-ID's tool is just one of the many examples of technology solving the problems of facial recognition. There are several AI researchers working on algorithms that fool facial recognition technology, like [PrivacyNet](#), [AnonymousNet](#) and [Fawkes](#). Most of these algorithms are adding for us invisible pixels to a face that mislead the recognition software.

In June 2020, The Black Lives Matter protests has rushed developers and platforms to build tools that protect the faces of protestors. On June 3rd, the secure messaging app Signal stated that "[2020 is a pretty good year to cover your face](#)" as they announced a new blur feature in their image editor for iPhone and Android devices, to help protect the privacy of the people in the photos users share. In the same week, San Francisco-based software developer Noah Conk released an [iOS shortcut](#) that automatically blurs faces and wipes all meta-data relating to GPS location, time and the camera with which the photo was taken. To create this tool, Conk used Amazon's facial recognition system Rekognition. Over the past years, government and law enforcement agencies have eagerly used Rekognition to identity suspects. Now the same software is also used to protect suspects.

Catogories we want to focus on:

How to distract facial recognistion:

- *Fashion*
- *Make-up*
- *Illusional prints/ that look like a face to facial recognition and algorithms*
- *Masks*
- *Tattoo covering*
- *Pupil covering/ lenses*
- *"adversarial" printed images*
- *thermal radiation for drones*

How to not be tracked

- *AI- Generated images or use of face-filters for your socials to stop the algoritm.*
- *Track and trace security, airplanemode etc.*
- *App for filming the protest with facial blur. To protect yourself and your fellow protestors.*
- *Knowledge of camera reconistion by a protest*

Protecting yourself from physical harm at the protest.

- *(Umbrella) for toxic liquids and gasses.*
- *Water*
- *Glasses*
- *Filming policemen*
- *EHBO kit*

Mask made out of vegan leather

<https://peeberpam-blog.tumblr.com/post/85647277596/this-kombucha-mask-is-almost-done-i-guess-it>

https://www.reddit.com/r/DiWHY/comments/ghseq7/made_a_kombucha_leather_face_mask/

https://www.boredpanda.com/sum-studio-cellulose-face-mask-from-bio-materials/?utm_source=google&utm_medium=organic&utm_campaign=organic

Hate mask

<http://sciencefashion.akbild.ac.at/blog/sturmhaube-hasskappe-hassmaske.html>

how to stay anonymous online

<https://www.csoononline.com/article/2975193/9-steps-completely-anonymous-online.html>

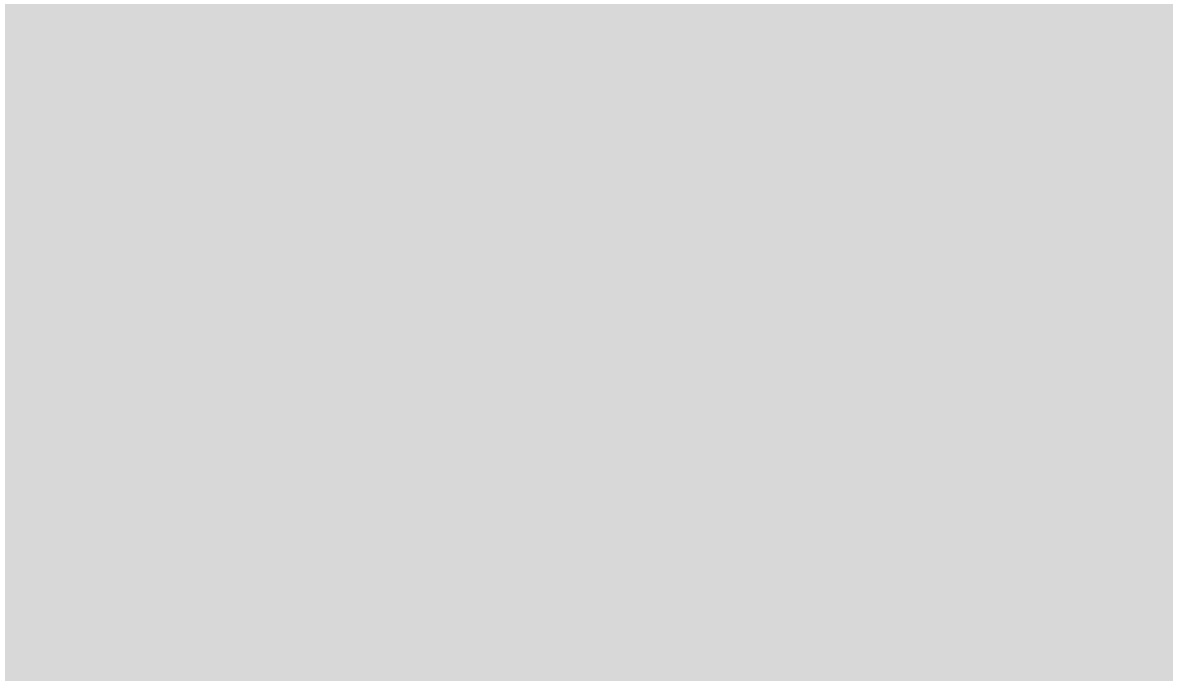
camera sensors interfere to prevent recording

<https://observers.france24.com/en/20190806-hong-kong-protesters-use-lasers-confuse-police-damage-cameras>

masks

<https://www.businessinsider.nl/clothes-accessories-that-outsmart-facial-recognition-tech-2019-10?international=true&r=US>

[How to Grow Leather-Like Material Using Bacteria \(Making Kombucha Leather\)](#)



Print:

