

Facial Recognition

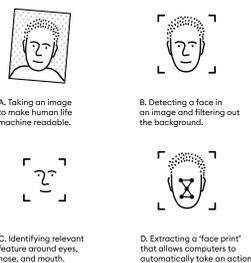
Low Tech Canvas Against High Tech Surveillance

Use our **wearable** guides to become a digital explorer of your city. See your neighborhood in a new light while exploring issues around facial recognition, voice identification, gait recognition, thermal imaging, and Wi-Fi tracking.

Be careful: becoming an explorer is exciting but at times jarring. You might learn more about your world than you want. Now take this canvas to the streets, bring your curiosity, watch, listen, and play. Try out some of our tactics and strategies to resist data collection in public space and co-design your neighborhood.

Getting a lay of the land

1. How computers capture a face



Why capture a face?

- To collect** a large set of images needed to train facial recognition technology.
 - To access** a device or service, e.g. Face ID to unlock an iPhone.
 - To match** the images of 'persons of interest' on police watchlists to faces in a crowd to enforce bans at stadiums and other public venues; to power biometric gates at airports.
 - To label a face** with characteristics like age, gender, expression, or emotions.
- These labels have been used to see if you are paying attention in church, or to target advertising based on your emotional state.

2. How comfortable are you with facial recognition?

Facial recognition is slowly entering our 'public spaces'. It is being tested by a range of actors from police to schools across Europe. How much do you trust these actors to use this technology? Listen to your gut, and write on this canvas how comfortable you are from **not at all** to **very**.

	Not at all	Very
Airport to go through e-gate	<input type="radio"/>	<input type="radio"/>
City for crowd management on street	<input type="radio"/>	<input type="radio"/>
Church to monitor attendance	<input type="radio"/>	<input type="radio"/>
Gym to authorize your membership	<input type="radio"/>	<input type="radio"/>
Police to identify 'person of interest'	<input type="radio"/>	<input type="radio"/>
Bank/ATM machine to verify your identity	<input type="radio"/>	<input type="radio"/>
Schools to verify children who enter the building	<input type="radio"/>	<input type="radio"/>
Stadium to match supporters with a stadium ban	<input type="radio"/>	<input type="radio"/>
Supermarket to ban known 'shoplifters'	<input type="radio"/>	<input type="radio"/>

3. Spot the camera

Facial recognition starts with cameras, which have been creeping up across town. Do you know how many there are?

Instruction: Walk through your neighborhood and spot the cameras. When you find one, check the box and take a closer look to figure out who owns them. Are there any markings, stickers or logos on it? Is there an information sign nearby that explains why it's there?

Spotter tip: To find a police van or drone with a camera, explore the area near a soccer stadium when there is a match, or a government building when there is a state visit, or a protest area.

Pro tip: Can you locate a sign that informs you about the purpose for which the cameras are used?

Where	Who	Why
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Locating camera surveillance

Highlight or color the areas on the map where you think camera surveillance is happening. Done? Scan the QR code and see where it is being implemented.

Pro spotter tip: Is this all? No, cameras used by police, companies or individuals are not included on the map.

Challenge: Do you live in a neighborhood without camera surveillance? Go to the streets and see if you can find cameras that are not included in your map.

slimmeapparaten.amsterdam.nl



6. Avoid being spotted by cameras

Camouflage yourself by using low tech tactics against high tech monitoring. Overexpose your face. Light up your face by attaching LED lights to your baseball cap.

- Materials:**
- Baseball cap
 - 10mm Diffused LED
 - 3V Lithium Batteries
 - Tape

Instructions:

- Step 1:** Place a LED leg on each side of the battery.
- Step 2:** Cut off tape and tightly wrap the tape 2-3 times around the battery and the LED legs.
- Step 3:** Tape the LED light to your baseball cap. Remember to break the asymmetry of your face by positioning the lights in random angles.

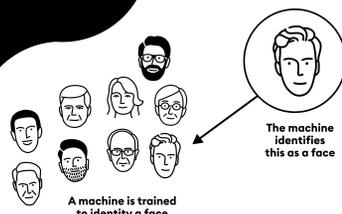
Tip: Overexposure will make you more visible to the human eye but less visible for cameras.



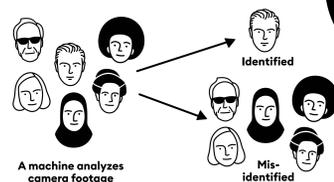
5. Bias at a glance

The Covid-19 pandemic shows how at times of crisis, public health and crowd management is often positioned as a trade off between health and privacy. These choices influence where and when camera surveillance and facial recognition are deployed and who it impacts. And this technology often comes with its own bias.

Groundbreaking research by Joy Buolamwini and Timnit Gebru shows how facial recognition products by IBM, Microsoft, and Face++ work best on white men and misclassify women of color. Explore these and more issues with facial recognition here. <http://gendershades.org>



A machine is trained to identify a face



A machine analyzes camera footage

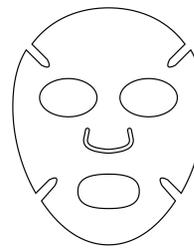
Navigating privacy in public spaces

7. Hiding in the crowd

Any mask will stop facial recognition from working, but people might look at you strangely when exploring the city in a Guy Fawkes or gorilla mask. URME Paper Surveillance Mask came up with the perfect solution now we can all wear Leo Selvaggio's face.

Pro spotter tip: Wear it with a baseball cap or beanie. How does it feel to explore the city in disguise?

Print your own by scanning this QR code and following their instructions.



URME Paper Surveillance Mask

8. Protecting your images online from facial recognition

Ever wonder what happens to your pictures after you post them online? Those building and using facial recognition have been spotted using online images to train their systems or match a 'person of interest' to those faces 'found' online.

These scientists created Fowkes, a tool to protect your identity while sharing your images widely. sendlab.cs.uchicago.edu/fowkes



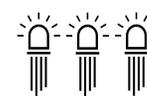
9. Make the invisible visible

Cameras are popping up around town and go unnoticed. They are so normalized that we stop seeing them. Make the 'invisible' visible, light up your neighborhood by creating these LED throwies and attaching them to your local surveillance location.

- Materials:**
- 10mm Diffused LED
 - 3V Lithium Batteries
 - Magnet
 - Tape

Instructions:

- Step 1:** Gather all the materials.
- Step 2:** Place a LED leg on each side of the battery.
- Step 3:** Cut off tape and tightly wrap the tape 2-3 times around the battery and the LED legs.
- Step 4:** Place the magnet on the + of the battery and continue to tightly wrap it. Congrats, you have now made your first throwie.
- Step 5:** The following action might not be advised in your political context, but if possible find a camera that is in throwing distance and toss you throwie at a surveillance camera.
- Know your context:** There might be sanctions on taking pictures of military or strategic areas, and protest could be places of tension.



Co-designing your digital neighborhood

Technologies evolve rapidly so it's important to move from low tech camouflage solutions to co-designing your digital neighborhood. Check out the Janosch Delcker experiment and see what works and what doesn't.

<https://tinyurl.com/JanoschDelcker>



Please remove my data

10. Exercise your rights

The European data protection bill has given us more control over what happens to our data. For example, you now have the right to access your data held by a third party, correct it if it's inaccurate, ask for it to be removed, or even move it to another platform.

Instructions:

Let's try how this works in a public space.

Step 1: Go to a public area like a station, stadium, or shopping street.

Fold this canvas so that the above message is showing. Walk in front of a camera holding it in such a way that it's visible on the image.

Step 2: Note down the exact location (any characteristics), time and date.

Step 3: Find out who is responsible for the cameras in this public space by looking for a logo or asking those who are responsible. This can be a sales or info person or you can even ask your local council.

Step 4: Approach the entity responsible for the cameras and ask for access to the image they captured of you. Include the location, time and date in the request.

Step 5: Ask if they can remove it.

11. There is power in numbers and opinions

The public space belongs to all of us. To imagine what your ideal neighborhood looks like, go out and talk to those you share it with. Approach a friend, neighbour or shopkeeper and start a conversation about privacy and facial recognition.



Q1: Have you seen any cameras in the street here?

Q2: Do you know who owns them and why they are used?

Q3: How would you feel if a shop would use facial recognition to identify you?

Q4: How would you feel if the police would use facial recognition to identify you?

Q5: Are there any locations in the city where you feel the use of facial recognition would be okay?

12. Join a community

The use of facial recognition is a complex issue. Don't go at it alone, find a community!

Pro spotter tip: Find your local digital rights group or crypto party and join their mailing list or meet ups. Unsure where to find them? Search for 'human rights and facial recognition' 'NGO + digital rights + your country'

You'll probably find groups like Bits of Freedom, EDR, Liberty, Ada Lovelace Institute, AI Now, Article 19, La Quadrature du Net, and Data and Society.

Support those fighting for your rights. Donate to your local digital rights or human rights group.

Colophon

Version Sept 2021 ENG V02

datawear.
www.datawear.it

Produced by Fieke Jansen, Data Justice Lab in collaboration with designcollective idiotēs with support from Designlab Digital City, Amsterdam.

Supported by **moz://a** City of Amsterdam **Hivos** **obc** **idiotēs** people united



Licence CC 4.0 Share and attribute alike Icons from the Noun Project