from print to pixel


# Facial Recognition

## What Can Machines Read in Our Faces and What Is This Information Used For?

fotomuseum winterthur

# OVERVIEW

## Facial Recognition – What Can Machines Read in Our Faces and What Is This Information Used For?

### Topic and Main Question

Facial recognition technology has come to permeate our lives over recent years – this could be when we put on an animal mask on Snapchat, unlock our smartphone with our face or go through automated passport control. The possibilities this technology offers are immense, ranging from identification and surveillance to the analysis of character traits. But the technology also raises some fundamental moral and legal issues. Who is watching or analysing whom, and for what reasons? How can people give permission to be watched – and do they even know they are being watched in the first place? How are machines trained? What mistakes can they make and what biases do they have? How can we use this technology in ways that are responsible and safe?

### Relevance

In order to navigate all of today's many media and information technologies, schools and teachers must consciously engage with the latest developments. The technology of facial recognition is a field that directly affects students in their everyday lives and involves a large number of moral, legal and social questions. Sensitising students to these issues and encouraging them to explore the questions they raise in a nuanced way will help them to form their own critical opinions and to make use of the technology in responsible ways. Students will also see contemporary art as a means to reflect on relevant social issues and initiate discussion of them.

### Structure

This workshop comprises three double lessons and is geared to topical examples from everyday life and contemporary artistic positions that address the theme of facial recognition. The first double lesson gives a detailed explanation of the concepts and terminology involved and looks at ways of sensitising students to the subject. The second double lesson presents the challenges posed by this technology as well as its areas of application and the ways it is used. In the third double lesson students look at the legal, activist and artistic strategies that they can use to outwit facial recognition, and they will test out their own creative solution in practice. The documentation includes lesson plans and worksheets for students as well as additional background information and further reading for teachers.

## Learning Goals

— Students become acquainted with the technology of facial recognition and its uses.
— Students work on background knowledge related to this theme.
— Students become acquainted with methods for protecting their own personal image data on the internet.
— Students discuss the potentials and challenges of this technology and form their own opinions based on critical thinking.
— Students become acquainted with contemporary positions that take a critical view of facial recognition. They experience art as a way of reflecting on contemporary social issues and initiating discussion of them.
— Students become acquainted with an activist use of images and explore this with their own creative approach.

School Level: Secondary I and II, ages 13–19

Themes: algorithms, artificial intelligence, big data, control, digitalisation, digital media, digital self-defence, discrimination, ethics, facial recognition, machine learning, media art, media competence, (self-) portraits, social media, surveillance, technology

# INTRODUCTION

The topic of facial recognition has recently been in the news a good deal and has generated considerable interest. Many people unlock their phones, go through passport control and use Snapchat filters – all thanks to facial recognition. Soon more facial recognition applications may be added, such as contactless payment. Looking at developments around the world, including the Clearview scandal in the USA and the surveillance of protestors in Hong Kong, we see a more problematic and questionable image of this technology. It is important for us to have a better understanding of how these technologies work, where they are already being used and the opportunities and risks that go with them. While they certainly offer a wide range of possibilities, there are moral, legal and sociopolitical questions associated with them that we need to discuss and respond to.

The technology of facial recognition comprises the detection, recognition and analysis of faces using digital methods. In the first stage, artificial intelligence (AI) detects where in the image a face is situated. We know this mechanism from cameras that detect and focus on faces and from cameras that can automatically track them. In the second stage, the AI application recognises the face on the image and identifies the person. This is used for surveillance or automatic tagging, of the kind found, for example, on Facebook. The third stage goes so far that the AI is able to analyse the face by comparing or linking the face it has recognised with additional information. In this way, emotions can be gauged, and there have been controversial attempts to predict age, gender identity, sexual orientation, origin and income. These analyses can be used for intelligent advertising banners.

And here we come to the issues that definitely require social and political debate. While the mere detection of faces is largely unproblematic, as soon as people can be individually identified, legal and moral questions come into play. Who is watching or analysing whom, on what basis and for what purpose? How can people give permission to be watched – and do they even know that they are being watched in the first place? In addition to this, AI technologies are not neutral, as they are so often said to be. Quite the contrary, they often contain very strong distortion or bias, partly due to imbalanced data sets used for the training of these artificial intelligences. Research has shown that important image data sets consist to a large degree of white (cis) male portraits. Moreover, these technologies are developed by humans and no one is completely neutral and free of bias.

The paradox behind the development of facial recognition is that we often ourselves provide the data that are used in the development and training of these technologies, but mostly without knowing this and without consciously or actively agreeing to it. It is therefore important to raise student awareness about the legal situation pertaining to the use of their data on the internet and to show them how they can increase their own security and protect their privacy.

# BACKGROUND INFORMATION

## Double Lesson 01
## What Is Facial Recognition?

### Zoom Pavilion


Rafael Lozano-Hemmer and Krzysztof Wodiczko, *Zoom Pavilion*, 2015,
3:52 min, Art Basel, 2016

### Work Description

*Zoom Pavilion* is an interactive installation by the two media artists Rafael Lozano-Hemmer and Krzysztof Wodiczko. It consists of projections on three walls, fed into by twelve intelligent surveillance systems. These use algorithms for facial recognition and have been trained for use on the audience. They recognise the presence of the participants and record their spatial relations within the exhibition space. On the basis of gaze and gesture, the system draws conclusions about how individuals connect with each other and the levels of interest and attraction between them.

In this work, the artists use an everyday technology and have the audience to interact with it. At first sight, the installation seems like an enormous playground perfectly suited to taking selfies. But here art is also used to ask social, legal and moral questions about our use of artificial intelligence. Who is watching whom and for what purpose? How do

people give permission for this? What further uses might be found for the information regarding the interests and relationships of the groups of people under observation?

*Zoom Pavilion* is the first collaboration between the artists Rafael Lozano-Hemmer and Krzysztof Wodiczko. For many years, the two have been examining ways in which their own artistic exploration of themes such as the public sphere, surveillance and control can be spatially experienced and presented to an audience interactively.
This work has already been shown in various international exhibitions and the video here was recorded at the Art Basel art fair in 2016.

> For further information on the project, see http://www.lozano-hemmer.com/zoom_pavilion.php

# Double lesson 02
# How Does the Technology Work, Where Is It Used and What Challenges Does It Entail?


Noah Levenson, *Stealing Ur Feelings*, 2019

## Project description

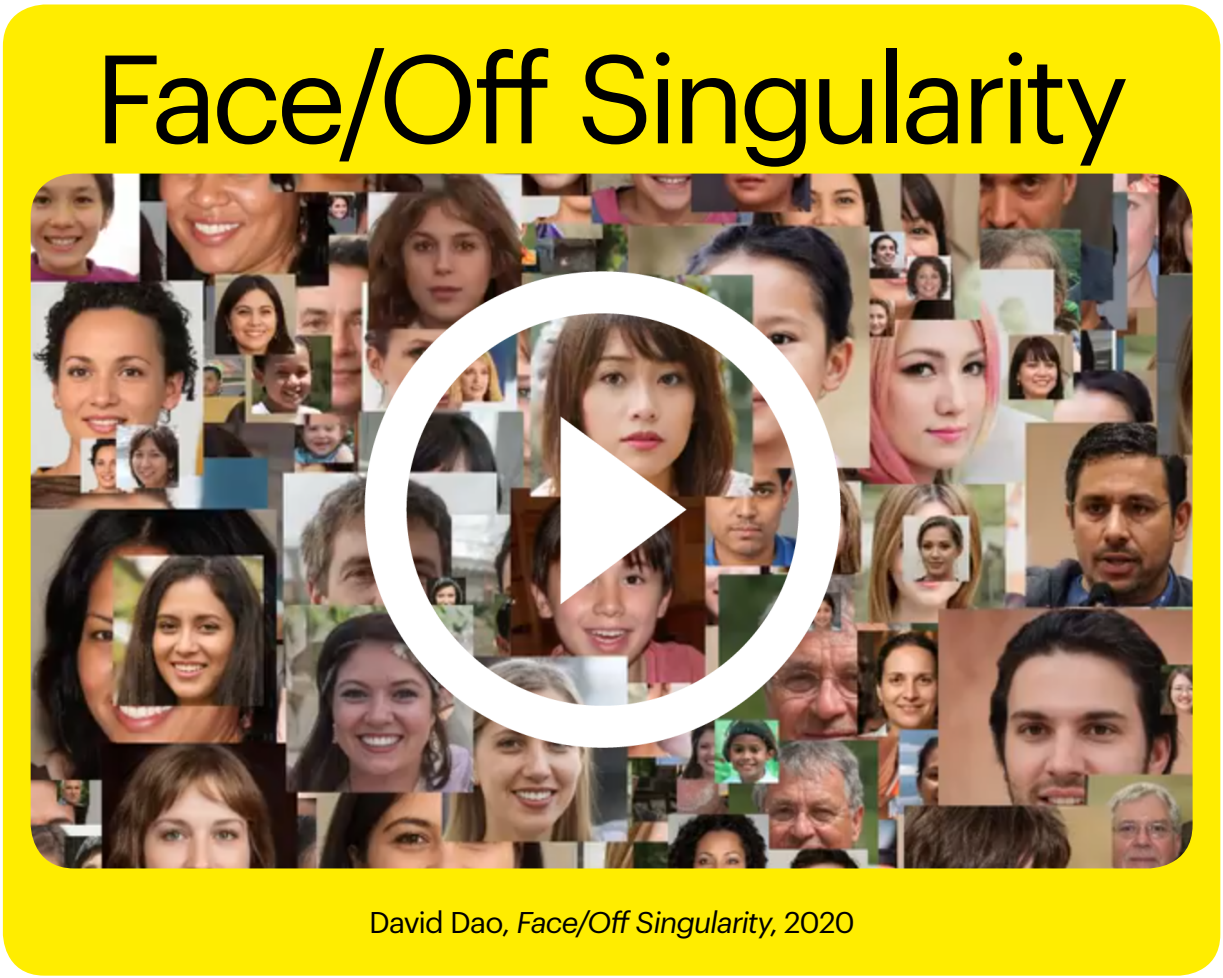
In 2018 US American programmer Noah Levenson developed *Stealing Ur Feelings*, a playful web tool that shows how the facial recognition behind many apps actually works and how these apps are able to use emotional analysis in order to make predictions and influence consumer decisions, while also attempting to draw conclusions about gender identity, sexual preferences, income, IQ and political views.
This interactive video was presented in various contexts, including at the Tribeca Film Festival and Tate Modern in London, and won the Mozilla Creative Media Award.

> For further information on the artist and the project, see https://www.noahlevenson.com/

## Operation of and Information on the Application

— This interactive video accesses the user's computer-integrated camera and analyses their face with the same technology used in Snapchat, Facebook and Instagram.
— To try this out, students must enter their permission in a dialogue field for the application to access their camera. (If this option is blocked on school computers, then the students will have to use their own devices or smartphones.)
— The video starts when you click on the smiley that appears.
— At the end of the video, the results can be downloaded as an image file.
— The video lasts about 5 min.

> Note: If you are using a smartphone, the video must be viewed in landscape mode.




David Dao, *Face/Off Singularity*, 2020

## Project description

Computer scientist David Dao conducts research at ETH Zurich into the ethical use of artificial intelligence (AI) and data systems for sustainable development. Dao's project is designed to educate people about facial recognition technology. In *Face/Off Singularity*, for example, he shows how users can take action against facial analysis using 'adversarial perturbations'. The web application modifies individual pixels in portraits in such a way that they remain recognisable to the human eye but not to machines. This enables users to protect their identity from automatic recognition.

The categorisations are in line with existing social biases and the constructs of 'gender', 'race' and 'sexual orientation' – which are deliberately intended to prompt critical reflection. Here Dao sets out to voice a critical view, on the grounds that the putative identification of sexual orientation could, for example, lead to an intensification of the discrimination and persecution experienced by many LGBTQIA+ people around the world. However, a Stanford University study (AI-based Gaydar) focused on the disputed physiognomic typing was scientifically discredited when it was shown that the researchers' deployment of AI was predicated on false underlying assumptions combined with normative and truncated views of possible life realities. This brings up further questions: In what other ways might this practice of facial recognition be detrimental? Are there categories that could be applied in facial analysis that are potentially less problematic?

> For further information on the study, see https://www.theverge.com/2017/9/21/16332760/ai-sexuality-gaydar-photo-physiognomy

Dao's software is based on 'FairFace', an image data set that seeks to disrupt the focus on white people by providing a more representative selection of images geared to the categories of 'race', 'gender' and 'age'. It turns out that the facial recognition software trained with this data set is much more accurate in analysing BIPoC (Black, indigenous and people of colour) than standard algorithms. This begs the question of the extent to which people with disabilities are disregarded and how much this image data set can be used for racialisation or is open to misuse by the authorities.

> Link to the data set used: https://arxiv.org/abs/1908.04913

> For further information on the artist, see https://daviddao.org/
> For further information about the project *Face/Off Singularity*, see https://www.fotomuseum.ch/en/explore/situations/157111
> For an overview of disturbing, unfair and discriminating uses of AI, see https://github.com/daviddao/awful-ai
> For a critical overview by David Dao on the opportunities and uses of KI, see https://medium.com/@daviddao/awful-artificial-intelligence-99b8220746c

## Information about the App and How to Use It

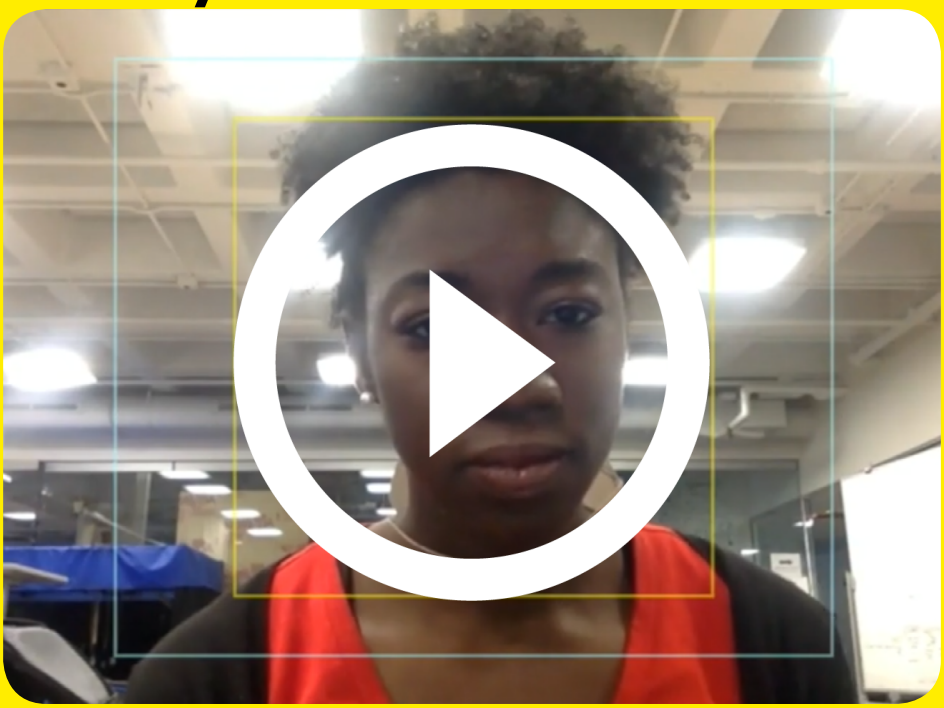
— To start the program, click on the 'Enter' button.
— In the next dialogue field, select the facial recognition algorithm; either the more accurate version 'EvilNet125' or the faster version 'FastEvilNet125'.
— Under 'Upload' you can now upload your own image.
— Choose the corresponding algorithm under 'Prediction Model' and then click on the 'Predict' button. The facial recognition software now makes an estimate and calculates its presumptions with regard to gender identity, age, skin colour, sexuality and the likelihood of criminal activity.
— In a next step you can use the 'Citizens' button to access the existing database or select the eye-button to generate a random hit.
— Under 'Adversarial Model' you can activate the distorting filters that make it more difficult for the software to analyse the images. The counter model developed by Dao can learn which pixels the algorithm requires to recognise the face, age and sex, and then changes these – they can be adjusted with the Epsilon (ε) controller – so as to confuse the algorithm.

## Data Protection Note

Protection of personal data is guaranteed when using this programme. No personal data leaves your own computer. All data remains on your computer and is stored there.

# Double Lesson 03
# How Can I Protect Myself from Facial recognition?

## Joy Buolamwini



Joy Buolamwini, TED Talk: *How I'm Fighting Bias in Algorithms*, TED Institute, 2017, 8:45 min

### Project description

The Ghanaian American computer scientist and activist Joy Buolamwini conducts research at the MIT Media Lab, where she identifies discriminating distortions in algorithms and develops solutions for programming. During her PhD dissertation, she worked with existing facial recognition software and discovered a problem. The software did not recognise her face, as the people who programmed the algorithm had not taught it to detect a broad range of skin tones and facial features. She calls the phenomenon of algorithmic bias in the field of machine learning 'the programmed gaze'. In her research, Buolamwini showed 1,000 faces to facial recognition systems and told the programs to identify if these were (cis) male or (cis) female. She ascertained that it was particularly difficult for these software systems to identify Black women and women of colour. Her project, *Gender Shades*, attracted a great deal of media interest and became part of her PhD dissertation at MIT. Her study *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, published in 2018, prompted IBM and Microsoft to fix this defect in their software.

Buolamwini's research sets out to highlight the biases of codes that can lead to people

being discriminated against. In this, she wishes to alert individuals and large software firms to the need for responsible programming. Her scientific study played an influential part in addressing sexist and racist prejudices in Google and Microsoft products and processes.

> Joy Buolamwini, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, MIT Media Lab, 2018: http://proceedings.mlr.press/v81/buolamwini18a.html

# Adam Harvey

Adam Harvey, *CV Dazzle*, 2010–2015

## Project description

The US American artist and researcher Adam Harvey lives and works in Berlin. His work deals with surveillance, privacy and computer technology. In his *CV Dazzle* project, he has developed a kind of modern camouflage that can protect us from facial recognition. The name is taken from a method that made use of cubist-inspired patterns to disguise the size and locations of battleships. It was used in World War I by the Royal Navy and the US Navy.

In similar ways he uses hairstyles and make-up to redesign the face, thereby interrupting the points of reference that facial recognition uses to detect human faces, such as symmetry, contours and the position of the facial features. The result is a fashionable 'anti-face'.

> For further information on the artist and the project, see https://ahprojects.com/cvdazzle/
> *Look Book*: https://cvdazzle.com/

# FURTHER LINKS AND LITERATURE

## Applications of Facial Recognition

This is how the automated passport control system works at Zurich Airport:
> https://www.swissinfo.ch/eng/society/biometric-id_zurich-airport-to-pilot-face-recognition-system/43504538

The use of surveillance cameras in retail trade is controversial in terms of data protection:
> https://www.cnet.com/news/with-facial-recognition-shoplifting-may-get-you-banned-in-places-youve-never-been/

Contactless payment based on the Amazon Go model:
> https://www.theguardian.com/us-news/2020/feb/25/amazon-go-grocery-supermarket-seattle-technology
> https://www.cirrusoft.com/2019/12/19/retail-future-no-lines-no-checkouts-no-cash/

Advertising video by Amazon Go:
> https://www.youtube.com/watch?v=NrmMk1Myrxc&feature=youtu.be

The use of personalised advertising is being tested in the public space:
> https://www.youtube.com/watch?v=B5eLmqSjfko

## How the Technology Works

Smartphones secured by facial recognition can be easily tricked:
> https://www.kaspersky.com/blog/face-unlock-insecurity/21618/

This is how the technology behind Snapchat filters works:
> https://medium.com/cracking-the-data-science-interview/snapchats-filters-how-computer-vision-recognizes-your-face-9907d6904b91

## Challenges and Problem Areas of Facial Recognition Software

In their book *Data Politics* (2019), the editors Didier Bigo, Engin Isin and Evelyn Ruppert explore arguments about data acquisition as a political concern:
> https://www.taylorfrancis.com/books/e/9781315167305

How simple it is to use profile images from the internet to identify people:
> https://eandt.theiet.org/content/articles/2020/08/how-online-facial-recognition-systems-could-endanger-our-personal-privacy/

Firms like the American start-up Clearview are collecting large amounts of face data from the internet and developing programmes for identification:
> https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
> https://podcasts.apple.com/us/podcast/why-clearview-ais-facial-recognition-is-privacy-nightmare/id1142790530?i=1000464215449

## Data Protection and Creative Protective Measures

Data protection and facial recognition technology:
> https://www.reputationdefender.com/blog/privacy/how-to-protect-your-privacy-from-facial-recognition-technology
> https://www.thedenverchannel.com/news/360/facial-recognition-technology-does-it-violate-privacy-or-protect-community-

In May 2019 San Francisco was the first city in the world to prohibit the use of facial recognition technology:
> https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

In 2019 protesters in Hong Kong developed creative precautions against intelligent surveillance systems – for instance, by styling their hair in such a way that it covered their face or by 'attacking' surveillance cameras with laser pointers:
> https://www.independent.co.uk/news/world/asia/hong-kong-protests-mask-ban-china-face-covering-hairstyle-a9145181.html?jwsource=cl
> https://www.buzzfeednews.com/article/rosalindadams/hong-kong-protests-paranoia-facial-recognition-lasers

# DOCUMENTS FOR SCHOOLS ON THE THEME OF FACIAL RECOGNITION AND DATA PROTECTION

## Data Detox Kit

Tactical Tech is an international NGO that works with citizens and civil society organisations to research the effects of the technology on society and to develop critical approaches:
> https://tacticaltech.org/

With the *Data Detox Kit*, Tactical Tech 2017 developed a tool for young people that can increase personal digital security and internet privacy using simple steps:
> https://datadetoxkit.org/en/privacy/essentials/

> Depending on the class level and the depth of inquiry required, these materials can also be used in double lesson 03.

# PLANNING GRID

Scope: 3 double lessons
Level: Secondary I and II, ages 13–19

### Learning Goals

— Students become acquainted with the technology of facial recognition and its uses.
— Students work on background knowledge related to this theme.
— Students become acquainted with methods for protecting their own personal image data in the internet.
— Students discuss the potentials and challenges of this technology and form their own opinions based on critical thinking.
— Students become acquainted with contemporary positions that take a critical view of facial recognition. They experience art as a way of reflecting on and discussing contemporary social issues.
— Students become acquainted with various ways of protecting their own images from facial recognition and implement one of these strategies using their own creative approach.

## Double Lesson 01
## What Is Facial Recognition?

| Time | Lesson phase | Contents | Tasks | Social form | Materials / Media |
|---|---|---|---|---|---|
| 20 min | Introduction | Sensitisation to facial recognition technology | **Worksheet I: Work Analysis**<br>Rafael Lozano-Hemmer and Krzysztof Wodiczko, *Zoom Pavilion*, 2015, 3:52 min, Art Basel, 2016<br>— Students watch the video: a first time to gain an impression of the work and a second time to answer questions on the work analysis in a follow-up discussion.<br>— Teacher presents additional background information on the artists and the work. | Plenary | — Projector / screen<br>— Worksheet I<br>— Background info on the work (Information for teachers) |
| 50 min | Digging deeper / Task | Explaining concepts and reflecting on the reading / Practically testing and experiencing methods of facial recognition | **Worksheet I: Defining Concepts**<br>— Read the explanation of concepts and understanding the differences between *facial detection*, *facial recognition* and *facial analysis*.<br>— Work through the tasks.<br>— Individual support from the teacher when testing the web applications *Stealing Ur Feelings* and *Face/Off Singularity*. | Pair work | — Worksheet I<br>— Own smartphone, tablet or laptop<br>— Background info on the two applications (Information for teachers) |
| 20 min | Conclusion | List opportunities and risks of the technology, followed by discussion and summary. | **Discussion / Reflection:**<br>— Collect views and assessments from the group task.<br>— Compare with first impressions from the video seen at the beginning of the double lesson.<br>— Summarise possible uses. | Plenary | — Worksheet II<br>— Board / flipchart |

# Double Lesson 02
# How Does the Technology Work, Where Is It Used, and What Challenges Does It Entail?

| Time | Lesson phase | Contents | Tasks | Social form | Materials / Media |
|---|---|---|---|---|---|
| 5 min | Introduction | Link back to contents of the last double lesson / Sensitisation to the challenges of the technology and its susceptibility to error, biases, discrimination and violation of privacy | Voting and discussion in plenary:<br>— Who can recognise a face more quickly and reliably – a person or a machine?<br>— The best facial recognition systems are much better and quicker than people. If we think back to the video *Stealing Ur Feelings* and the application *Face/Off Singularity* and review the insights from the last lesson, why should we not let the machines make decisions for us? | Plenary | — Board / flip-chart with the results from the last double lesson |
| 30 min | Further work / Digging deeper | Becoming acquainted with fields of application for facial recognition, and forming one's own opinions about this | Worksheet II: Fields of Application<br>— Reading and video insights into fields of application<br>— Work through the task. | Individual work | — Worksheet II |
| 45 min | Task | Seeing the problems in facial recognition and designing plans of action to counter them | Worksheet III: Operational Analysis and Challenges<br>— In groups, the students look at one example and discuss the problem presented there<br>— Read the additional info on the case study presented.<br>— Develop a plan of action: What must be changed so that the technology can be programmed to be more unbiased, fairer and less prone to error?<br>— Students present the problem and their plans of action to other students. | Group work | — Worksheet III a/b/c<br>— Smartphone or laptop<br>— Writing materials and paper |
| 10 min | Conclusion | Presentation / Reflection | Exhibition and Key Learnings<br>— Exhibit the plans of action<br>— Each student formulates one moment of personal insight from the lesson. | Plenary | — Plans of action |

# Double Lesson 03
# How Can I Protect Myself from Facial Recognition?

| Time | Lesson phase | Contents | Tasks | Social form | Materials / Media |
|---|---|---|---|---|---|
| 5 min | Introduction | Link back to the last double lesson<br>Collecting ideas for how to protect oneself from facial recognition | Brainstorming<br>In the first double lesson we got to know the challenges of the technology: What are they? (Susceptibility to error, discrimination and violation of privacy)<br>What can we personally do to protect ourselves from facial recognition and access to our data?<br>— Looking again at the plans of action, further idea collection | Plenary | — Plans of action<br>— Board/flip-chart |
| 20 min | Further work | Becoming acquainted with the legal situation and activist artistic positions that have developed strategies for protecting you from facial recognition | Worksheet IV: Protective Measures<br>— Reading<br>— Working through the tasks. | Individual work | — Worksheet IV<br>— Laptop / smartphone |
| 45 min | Practical application | Creating your own distorted self-portrait | Camouflage Look à la Adam Harvey<br>Let yourself be inspired by Adam Harvey's *Look Book*. Create your own covered or distorted portrait of your face, with the aim of preventing it from being identified by facial recognition software. Use make-up, style your hair or stick things on your face. Take photographs.<br><br>Additional Task:<br>— Consider what a clever social media post might say in order to draw your friends' attention to the subject of facial recognition. | Pair work | — Party make-up<br>— Hairspray<br>— Hairpins<br>— Decorative elements<br>— Make-up<br>— Make-up remover<br>— Face cloths<br>— Cotton wool pads<br>— Smartphone<br><br>— Perhaps set up a photo studio with a neutral background and good lighting |
| 15 min | Presentation | Presenting images | Presentation / Jury<br>— The pictures are shared in a class chat room and the most original is selected!<br>— Alternative (for demanding classroom dynamics or the danger of bullying): Students send their pictures to the teacher, who then projects them. | Plenary | — The photos taken in class<br>— Smartphone<br>— Perhaps projector and adapter (if required) |
| 5 min | Conclusion | Reflection | Feedback<br>— What have I learned about the subject?<br>— Where would I like to be more careful in future? | Plenary | |