FACEPOT

DOMINIK
SZAKACS

FACEPOT

Imprint

Bachelor Thesis 2020
Title: FACEPOT
Author: Dominik Szakacs
Matriculation-Nr.: 17-683-152
Date: June 2020

Academic Editor: Dorothy Kok

Typeface: Roboto Mono, Neue Haas Unica Pro

DOMINIK
SZAKACS

ABSTRACT

In recent years, artificial intelligence (AI) has become increasingly relevant because of technological progress. Without being fully aware of it, it influences our lives more than ever through increasingly complex algorithms. The increasing spread of facial recognition systems, especially in commercial applications, is changing the meaning and value of the human face.

The BA thesis examines the implications of this development in terms of society and the relationship between such systems while provoking ethical and moral questions. It focuses primarily on biometric facial data by exploring different approaches based on research and conclusions that resulted in a web application with a critical design approach.

ACKNOWLEDG-MENTS

At this point I would like to thank all those who supported and motivated me during the preparation of this bachelor thesis:

Andrés Villa Torres
Claudia Buck
Colin Schmid
Dorothy Kok
Dr Marcel Blattner
Florian Bruggisser
Gabriel Bach
Gavin Armstrong
Jérôme Krüsi
Joëlle Bitton
Jürgen Späth
Matthias Kappeler
Nicole Foelsterl
Peter Rohrer
Verena Ziegler
Parents and Friends

TABLE OF CONTENTS

INTRODUCTION

We face historically unprecedented ethical challenges due to technological progress, especially in the field of artificial intelligence (AI). Many applications already influence our daily lives, without us even being aware of them. This prompted me to apply this thesis to examine the risks and the opportunities in the field of computer vision.

As facial recognition becomes more widespread, especially in commercial applications, concerns about security, privacy, misuse, and errors are growing. Users may be giving away more than they intend to. The delusion of facial data collection is changing the meaning of the human face dramatically. It can be seen as a new type of currency. Therefore, a photo of a person is no longer just a photo. It is a defining feature of an identity that can be shared or used in ways that consumers might not understand, anticipate, or consent to. In serious contexts, it can be used to develop ethically questionable technologies.

Thus, I set myself the goal of conveying the vulnerability and current handling of biometric facial data to a wider audience in a provocative, playful, and accessible way. In this manner, my work attempts to raise people's awareness and to stimulate discussion and scepticism about the current legal status of facial recognition technologies.

As a prospective interaction designer, I selected this relevant topic and attempted to combine this immaterial technology with tangible experiences – to make the invisible visible. The topic will particularly affect emerging designers and cause them to remain cognizant of their responsibility, to think in all categories, and to consider the consequences.

I RESEARCH FIELD

BACKGROUND AND CONTEXT

ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence cannot be avoided. It appears to be the latest trend, although the idea of artificially imitating human abilities is hundreds of years old. Already in ancient times, in Greek and Egyptian myths, they fantasized and speculated on mechanical and artificial beings. The Dartmouth Conference in 1956 marked the official birth of artificial intelligence as a discipline. At the end of the 1950s, important programming languages such as FORTRAN, COBOL, or Lisp emerged, which contribute significantly to the development of artificial intelligence.

With the combination of the worldwide networking of man and machine, the exponential growth in computational power, and the storage and processing of vast amounts of data, the 21st century is revolutionizing this technological achievement.

Artificial intelligence is a complex subject and, therefore, there are many definitions. Below are two simple definitions:

> *The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision making, and translation between languages (Google, 2020).*

> *Artificial intelligence is software or a computer program with a mechanism to learn. It then uses that knowledge to make a decision in a new situation, as humans do. The researchers building this software try to write code that can read images, text, video, or audio, and learn something from it. Once a machine has learned, that knowledge can be put to use elsewhere (Dave Gershgorn, 2017).*

In recent years, AI has become increasingly integrated into our everyday life. We already use artificial intelligence every day without being aware of it, although the increasingly complex algorithms influence our lives more than ever. This technological progress probably presents us with historically unprecedented ethical challenges. Society should consider the relationship with intelligent systems to question the implications, opportunities, and risks behind them and, therefore, it is important to understand the different concepts of AI to ensure that artificial intelligence serves everyone and not just a few.

> *AI technologies are now beginning to offer the ability to see (computer vision), hear (speech recognition), and understand (natural language processing) more than ever before. While all three of these sensing capabilities will be important, computer vision may be the most significant, as it offers the most beneficial use cases for things like self-driving cars, facial recognition, and powerful robotics (Lasse Rouhiainen, 2018, p. 28).*

COMPUTER VISION (CV)

Seeing plays a fundamental role to interact effectively and efficiently with the environment. Therefore, it is undoubtedly the sense on which humans rely most and, therefore, is one of the most important senses of man (E.R. Davies, 2018, p. 1).

Lawrence Gilman Roberts' 1963 thesis "Machine Perception of Three-Dimensional Solids" is considered the origin of computer vision. His research was later expanded by MIT's MAC project. Professor Marvin Minski, one of the founding fathers of the field of artificial intelligence and the then director of the MAC project, believed that computer vision could be solved as a summer project of an MIT graduate. He had completely underestimated it, and even now, various aspects of computer vision are still being studied. In the 1970s, David Marr, an MIT neuroscientist, based his work on a study of the cerebellum, hippocampus, and human perception cortex, and laid the building blocks for modern computer vision and is, therefore, considered the father of modern computer vision. In summary: To a certain extent, computer vision functions in a similar way to human vision. Therefore, human vision is considered a source of inspiration.

> *Computer vision is a field of artificial intelligence (AI) that enables computers and systems to derive meaningful information from digital images, videos, and other visual inputs — and take actions or make recommendations based on that information (IBM, 2020).*

Computer vision is a branch of artificial intelligence that enables computers to interpret and comprehend the visual world. Computer vision has long been an integral part of our everyday life and is behind many seemingly banal technical applications. It can be found, for example, in barcode scanners at supermarket checkouts, in military combat vehicles, surveillance cameras, self-driving cars, our smartphones that are equipped with biometric identity authentication features, in photo and video cameras, and even in our printers to prevent the counterfeiting of banknotes.

> *Recent advances in the field of computer vision are leading to novel and radical changes in the way we interact with computers. It will soon be possible to enable a computer linked to a video camera to detect the presence of users, track faces, arms and hands in real time, and analyse expressions and gestures (Cambridge University Press, 1998).*

This prognosis has been confirmed during the last 20 years, and this progress will continue to advance, further changing the way we interact with computers with human-like visual capabilities. The accuracy of computer vision has improved considerably in recent years so that they can see and interpret with ever-increasing precision, and in some areas, they already outperform humans.

MACHINE LEARNING (ML) AND DEEP LEARNING (DL)

Learning is something quite natural for humans and is far more than just being dependent on data. We have an innate intuition that is passed on generationally through DNA. The way humans see things is different from the way a computer sees things. Both have their advantages and disadvantages depending on the field of application. Moreover, merging the two "views" could be the key to new applications, taking vision (input) and decision (output) to a new level, which might be beyond our imagination.

To understand the difference between machine learning and deep learning, it is crucial to know that deep learning is a subset of machine learning, which in turn is a subset of artificial intelligence (Grossfeld, 2020).

Machine learning uses algorithms to analyze data, learn from that data, and make informed decisions based on the learned data (Velykholova, 2018). In deep learning, which began to take off in 2012, algorithms are structured in layers to create an artificial neural network (ANN) that can learn and make autonomous decisions without human intervention. The design of an artificial neural network is inspired by the biological neural network of the human brain and leads significant gains in performance and accuracy compared to machine learning (Grossfeld, 2020).

> *If you want to teach a [deep] neural network to recognize a cat, for instance, you don't tell it to look for whiskers, ears, fur, and eyes. You simply show it thousands and thousands of photos of cats, and eventually, it works things out. If it keeps misclassifying foxes as cats, you don't rewrite the code. You just keep coaching it (Wired, 2016).*

As a result, the deep learning method is rather "data-hungry". It needs vast amounts of data for training and a significant amount of computational power. Therefore, data is considered the fuel of the future (Grossfeld, 2020). Massive amounts of data are being produced today and according to the futurist and computer researcher and pioneer of optical character recognition (OCR) Ray Kurzweil, $1000 worth of computational power will be the equivalent of a human brain in this decade. Year by year, the computational power increases exponentially.

Despite all the fascinating developments, the field of computer vision should specifically address the problems currently associated with it, such as bias, risk unawareness, and lack of explainability. Since each of us is unconsciously confronted with this technology daily, it is necessary to understand it at a certain level.

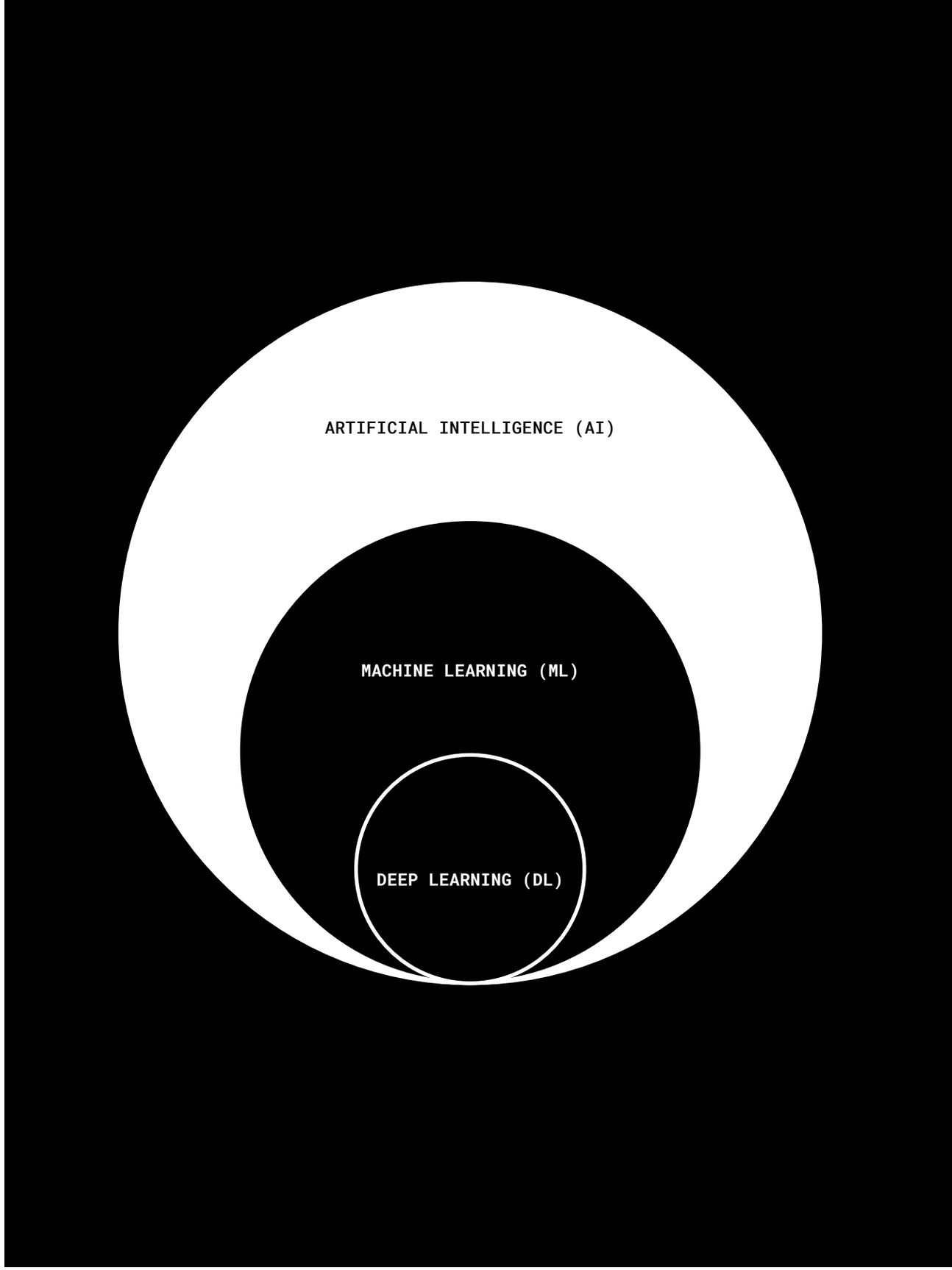

Figure 1. artificial intelligence, machine learning and deep learning (Source: Own representation based on Nadja Berchane, 2020)

METHODOLOGIES

MEDIA

To familiarize myself with artificial intelligence in a future scenario, I watched various films (Her, Blade Runner, Ex Machina, 2001: A Space Odyssey, Bicentennial Man, Tron, and The Imitation Game) during the spring holidays to ascertain the opportunities and risks of the rapid development of AI in a different way. I also played the interactive film Detroit: Become Human, in which human-like androids develop irrational behaviour and begin to question themselves. However, during the initial phase and through discussions, I realized that a possible and too speculative problem that lies in the distant future is quite elusive for people. Therefore, after the first mentoring, I decided to define the direction and the research question in a clearer and more contemporary way so that my project is immediately accessible to the masses. The term computer vision helped me to do this because we are exposed to this technology every day and even use it actively ourselves to some extent without being aware of it.

This kind of research should not be underestimated or devaluated, as it can inspire while offering insight into the topic: Experiencing ideas and possible situations visually and understanding them on a different level. Therefore, I will watch some explanatory videos on the topic of computer vision as well as recommended documentation regarding the impact in our society.

INTERVIEWS AND TALKS

Regarding the chosen methodology, I talked to several people during the concept seminar about their relationship with their computer. Since we are surrounded by computer systems in daily life and currently live in the “Big Data Era”, and since artificial intelligence is one of the fastest developing areas of human technology, my research must determine how experts and non-experts (users) perceive the situation, especially in the field of computer vision.

LITERATURE

To explore computer vision in detail, I have compiled a list of literature so that I can form a deeper understanding. It covers the following areas while focusing on computer vision: human-machine interaction, fundamentals, algorithms, applications, techniques, and learning methods. During the process, certain books were also recommended, in that the technology was more society-oriented rather than technical (see Books on page 88).

EXPERIMENTS AND PROTOTYPES

In the initial phase, I wanted to investigate the relationship between man and machine with small experiments. My research question was not concrete at that time, but I attempted to narrow down the subject by quick experiments. With the help of discussions and feedback, I could analyze the results to question them. They also provided visual support to explain and define the goal of my work so that it could be more specific, socially relevant, and contemporary (see Experiments on page 52).

After defining the final research question, I continue to use various prototypes and interventions to find ways to sensitize people to the current topic of facial biometric data. I would like to offer them the opportunity to understand and reflect on the facial recognition technology provocatively and experientially. I will investigate these prototypes during the concept and project development phase with people, and then build upon them (see Prototypes on page 56).

RESEARCH QUESTION

How can I convey the implications of biometric facial data to a wider audience in a provocative, playful, and accessible way?

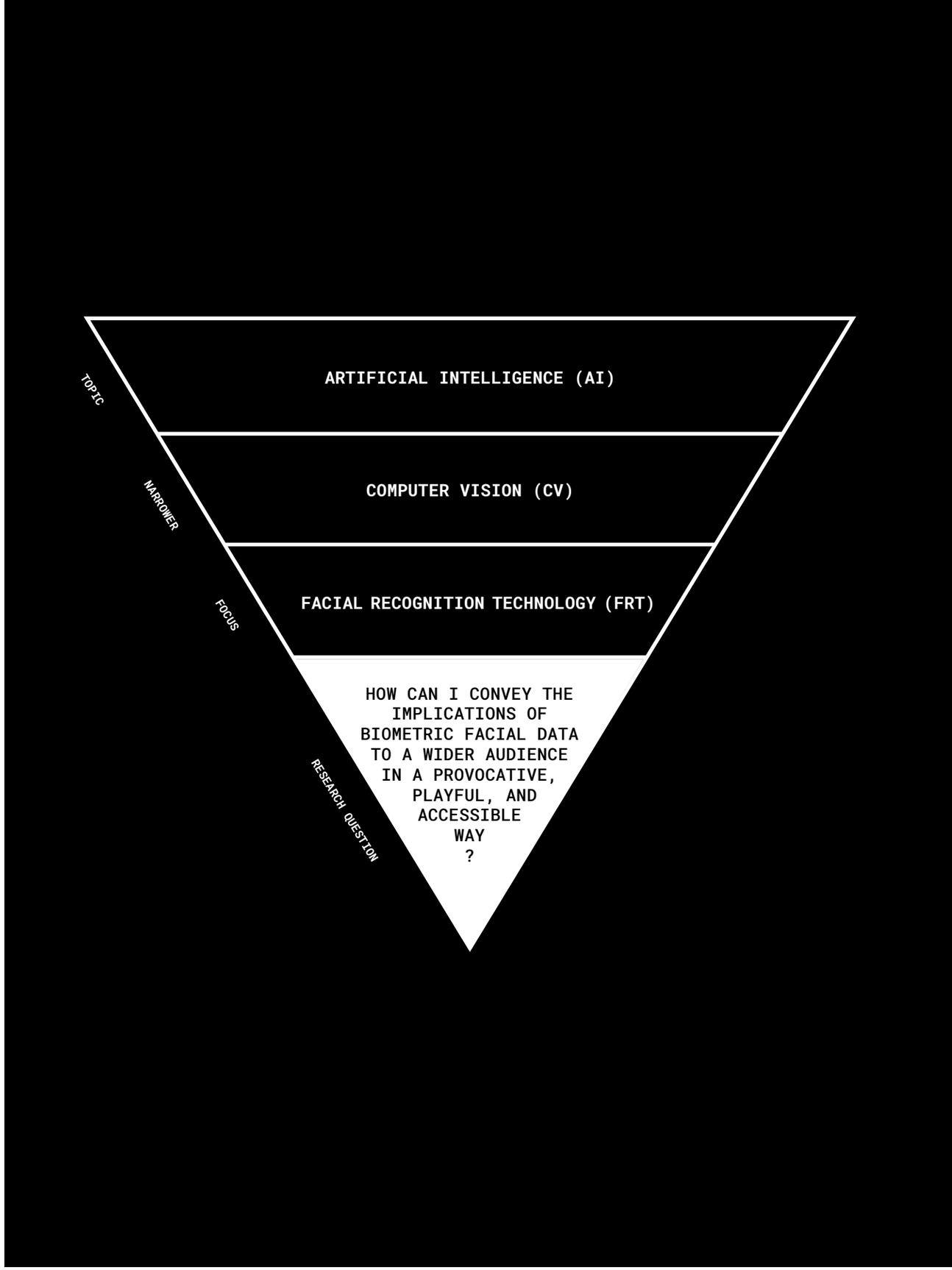

Figure 2. What makes a good research question? (Source: Own representation based on Chad Flinn, 2018)

MOTIVATION AND INTENDED CONTRIBUTION

Fei-Fei Li, a well-known personality in the field of computer vision, states the following: *"If we want machines to think, we have to teach them to see".* This was so inspiring and I wanted to address this unusual topic. Computer vision-based technologies are an integral part of daily life and have been widely adopted over recent years without us being aware of their presence. Facial recognition technology is one of the most controversial computer vision-based technologies that I feel committed to exploring during my bachelor thesis.

My motivation for my bachelor thesis work is to find out how I can entrust a broad mass with this steady growing technology without overtaxing them, for instance, with mathematical formulas. I want to pursue this goal because, in recent years, many commercial applications have begun to use face recognition technology, especially since the increasingly high-resolution cameras are present in practically every device.

Such achievements raise ethical questions and relationships of such systems. Therefore, society should be informed about the implications, opportunities, and risks in order to understand the concept or view of facial recognition technology, for example, to critically question a possible scenario of the abuse of this unknown power by companies and governments on a high level due to the lack of awareness and understanding.

> *Just as you can learn nothing about how the actual restaurant works by taking apart the drive-thru's microphone box, the pixels on a computer screen don't tell us anything about the computational machine that it is connected to. Contrast that with cracking open the hardware you're running that app on—although its internals would be a bit confusing, you would still find the screen, the battery or power supply, and a few other recognizable parts. That's because when it comes to something that exists in the physical world, you can touch and understand it, to a degree, when you crack it open. Machines in the real world are made up of wires, gears, and hoses that kind of make sense, whereas machines in the digital world are made up of "bits" or "zeroes and ones," which are completely invisible (John Maeda, 2019, p. 17).*

As an interaction design student, I have the opportunity to combine an intangible technology into tangible experiences, to make the invisible visible. I also want to take the opportunity to make this complex technology more accessible to everyone by interacting with it on an experiential level. My challenge is, therefore, to create a level of empathy and understanding that is effective and provocative but playful at the same time.

"I hear and I forget. I see and I remember. I do and I understand" (Confucius, 551 BC - 479 BC).

I am hoping that it will help to create new relationships, openings, and connections especially for people who are not specialists in this field, so that they can critically evaluate facial recognition technology inherent in the growing number of commercial applications.

II

CONCEPT

FIELD RESEARCH

FACIAL RECOGNITION TECHNOLOGY (FRT)

The face is a crucial part of the human experience. Our face is fundamental to the human ability to recognize a person as well as to communicate. It is the most vital form of identification, more so than our signature, fingerprint, or our voice.

While living beings can recognize and assign faces, non-living constructs can do the same – on an increasingly accurate level because of technological progress. A face contains much information that is unique to an individual and, therefore, we consider the application of facial recognition very personal. Facial recognition technology is considered by Techopedia as, *"a biometric software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's facial contours."*

A common definition of a biometric is an *"automatically measurable, robust, and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual" (Woodward et al. 2003: 1).* Therefore, facial recognition is one of many known biometric data types, such as iris recognition, fingerprint recognition, voice recognition, and, more recently, behavioural recognition.

Throughout the biometrics field, several terms are used interchangeably, especially concerning facial recognition and detection. While the terms may seem similar, there are some major variations, and it is important to consider these differences because they influence the use and application of these terms. Although the two are inseparable, there are some significant differences. The main difference is that face detection refers to a system that detects the presence of a face. Facial recognition also can recognize and identify the detected face based on a match stored in a database.

There are various face recognition techniques. However, the most common face recognition systems are based on the multiple nodes on a human face, which measure the values against the associated variables (Techopedia, 2020). However, the general functioning remains similar. With this technique, it is, therefore, possible to efficiently and accurately capture facial data and to identify the target person.

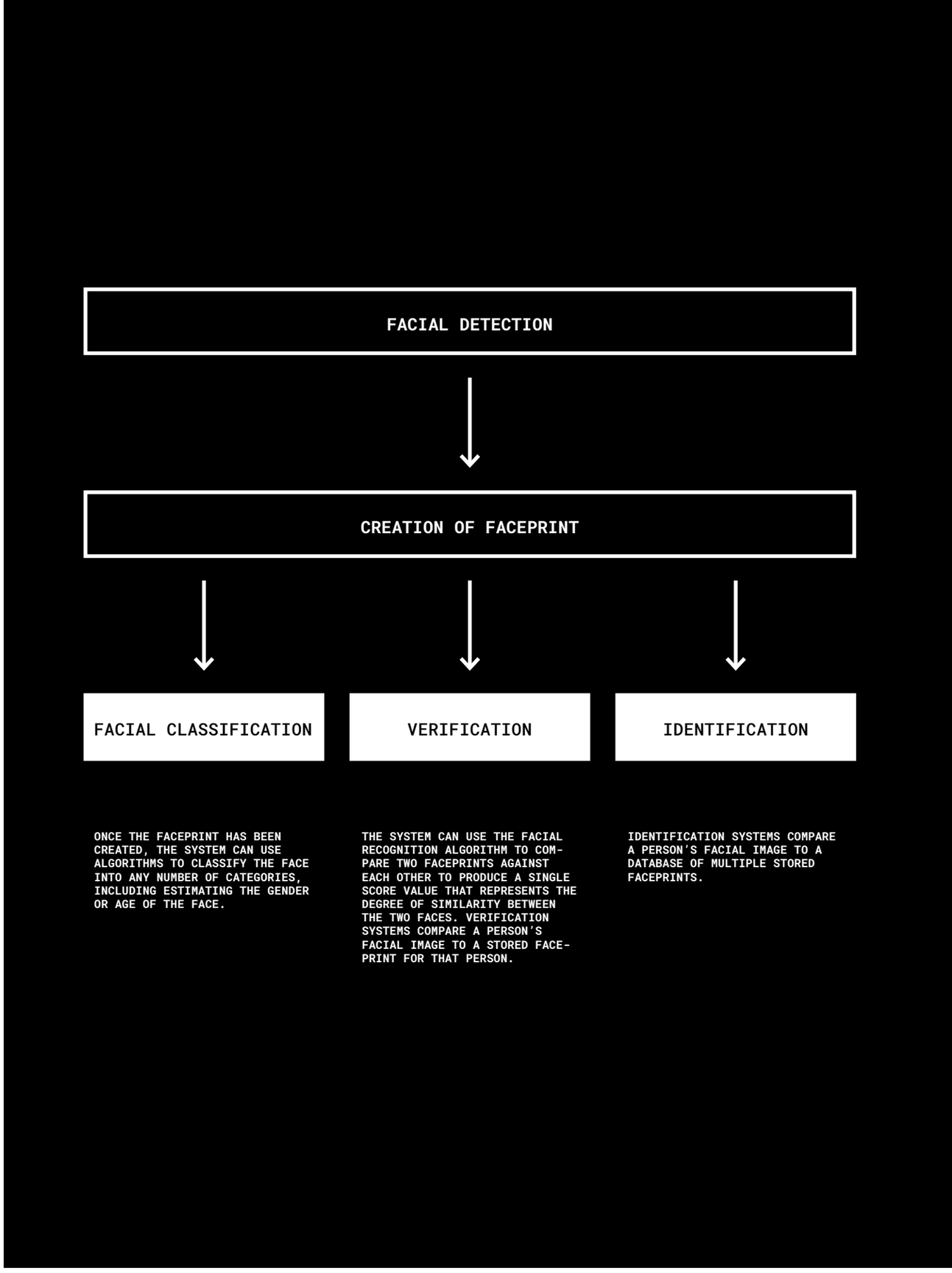

Figure 3. How Facial Recognition Technology Systems Generally Work (Source: Own representation based on GAO-15-621, 2015)

Generally, a functioning face recognition system requires four basic steps. First, a camera detects the face with the help of a face detection algorithm. Second, a photo of the face is captured and analysed by measuring the geometry of the face (a certain number of nodal points or landmarks). Third, the result is converted into a mathematical formula called faceprint (or facial biometric data), and at the end, it is compared to a database of stored faceprints, which then usually returns with attached pieces of information.

Many applications are already in use and influence our daily life without us knowing. We unlock our devices with our face as a password substitute, at the airport border control the face is automatically compared with the passport, and security in public places is increasing at the expense of personal privacy. However, these are not the only applications that are already in use. Many other new applications will emerge and change the world and the way we interact with it.

The popularity of this technology can be attributed to its convenience and efficiency as it is passive and non-intrusive. In other words, the analysis and evaluation of the face take place without any direct intended interaction with the person. Therefore, in the age of digitalization and globalization, it serves as a new form of knowledge and power that should not be underestimated or even ignored. Therefore, it should be ensured that this technology is used responsibly and appropriately to minimise the trade-offs and costs.

Due to the increasing adoption of facial recognition, especially in commercial applications, concerns have been raised about security, privacy, misuse, and errors. Users may give away more than they intend or, in the worst case, are not even aware that their facial biometric data is processed without their consent. Questions arise such as the following: Where is facial biometric data stored? Who can access it? What it is used for?

Facial recognition technology brings with it security and privacy issues. Government agencies and corporations could monitor and evaluate an individual, which removes an individual's anonymity. The technology could also lead to stalking or harassment if, for example, a private individual collects and uses facial data to find out who the person is. A kind of "Shazam" for faces instead of music, which could work with Facebook, for example, or dating platforms to gather information about the victim. Therefore, one's facial data could be collected and stored without any consent or knowledge, by virtually anyone with prior knowledge in the field, using open-source computer vision libraries.

Moreover, this offers new ways for criminals to access and steal the stored data to misuse or sell it. The prevalence of facial recognition technology is creating new incentives with harmful intentions and, therefore, dangers.

Furthermore, the accumulation of data breaches often ends up in the public domain. This proves that databases can be vulnerable and, therefore, never ensure full protection. A massive breach was reported on 26 February 2020 by the controversial facial recognition company Clearview AI. They claimed that the entire customer list, many of which were law enforcement agencies, had been stolen. Clearview AI has a database of over three billion photos from popular social media networks such as Facebook, Twitter, YouTube, Venmo, and LinkedIn.

You are the owner of your face. The image or the facial data, in turn, this property right is abandoned when facial recognition is used consciously or unconsciously. As there is a growing trend in the consumer sector to unlock personal devices using biometric technology, making traditional passwords obsolete, it can be concluded that facial data is more vulnerable. You can change a stolen password anytime and several times, but not something that is yourself. It is quite paradoxical to protect personal data with an even more personal format.

Mistakes in identification occur in practice, for example, due to poor lighting conditions or image quality, which leads to incorrect matching of the face with the database, resulting in mistaken identity. It can be concluded that this also does not provide fully accurate results and can lead to bias. A mismatch in face recognition can even ruin a life, which Steve Talley from Denver, Colorado experienced first-hand. He was charged with a bank robbery he did not commit because his facial data matched the suspect on the security camera footage.

Obviously, as with any other technology, there are also opportunities, but according to my research thus far, the risks outweigh the benefits.

KÜNSTLICHE INTELLIGENZ: PERSPEKTIVEN UND VISIONEN

[Translation by the author: Artificial Intelligence: Perspectives and Visions] The renowned German physicist and science journalist Ranga Yogeshwar held a talk on artificial intelligence on 3 March 2020 as part of the Tuesday evening lecture series of the Department of Industrial Design at the Zurich University of the Arts.

He asks and answers the most important questions around this topic and shows what will change and what will remain a pure utopia. He pointed out several times that we are undergoing a profound change because of the progress of artificial intelligence, which will fundamentally change our everyday life. All areas will be affected, such as medicine, work, mobility, economy, and communication.

In one example, Yogeshwar mentioned a student from Stanford University, who has the potential to replace an entire guild of radiologists who have studied for decades. With the help of machine learning and artificial neural networks, the student has been able to detect tuberculosis in X-rays with a very high degree of accuracy and speed. Since X-rays are data, just like normal images, he mentioned that it could be adapted to any application, such as facial recognition technologies, for example, to ascertain a person's identity.

Another example mentioned by Yogeshwar entails the help of an acceleration sensor in the common smartphone models, which can detect and process, with mathematical precision, a person's precise movements while walking. Slight, characteristic irregularities could indicate that a person is suffering from an early stage of Parkinson's disease. According to Yogeshwar, we are entering a world where we have to understand that data is different from what politicians think it is. It is much more complex than assumed. We are completely naive in our society, because we do not understand it or because we lack knowledge and awareness. From his perspective, it is not just about addresses or geodata, but it is about far more of what happens behind the scenes, without any notion from the user.

At the end of the presentation, he mentioned that we are moving into very exciting times because we are the first generation in the history of humankind that is able to change the world through innovation. Therefore, we can predefine something in terms of design but we should always bear the responsibility and impact in mind and think in all categories.

NEURONALE NETZE UND DAS BLACK BOX PROBLEM

[Translation by the author: Neural Networks and the Black Box Problem] On 26 March 2020, the ai-Zurich conference on artificial intelligence in business took place in a live stream. The talk by Dr Marcel Blattner drew my attention and I was able to follow his talk live online.

Dr Marcel Blattner studied physics and mathematics at the University of Zurich. As a chief data scientist at Tamedia AG, he is responsible for the development and implementation of complex data analyses that generate direct benefits for all stakeholders.

At the beginning of the presentation, he addressed the neural networks that have repeatedly led to breakthroughs in computer vision or speech processing in recent years. He highlights the problems of the connectionist approaches, as it does not understand the network and exactly how a particular decision is made. Therefore, it is mostly not interpretable by humans because the rules are based on abstractions created by machines. Unlike systems where the questions and answers are hardcoded, one understands how and why the network reacts to a given input.

He uses the car brake as an example: While he does not understand exactly how the mechanical process works, experts in this field do. He says that the disinterest of this black box arises because we assume that the institutions or people make the necessary checks to ensure that these systems function correctly. We trust that the manufacturers or the developers of these systems ensure that they do what they are made for and do it with care. Therefore, it is important not to blindly trust an AI system, because it is still not understood exactly how and what kind of concepts such systems learn.

Blattner also showed a very interesting example of a common object classifier, where a strange picture can confuse and lead to a completely incorrect classification. He claims that it is possible to systematically deceive such systems and lead them to produce false results. I realize at this point how fatal and dangerous it could be, depending on the application. One

should, therefore, not blindly trust a system, especially not if the functioning and the effects, are not well understood.

SURVEY

To obtain information in the field of computer vision, I applied the survey method as primary research and then evaluated the available data in the secondary research to gain decisive insights into the field.

To better assess the preference and expertise in this area, I surveyed with Pollfish, an online survey platform, with exactly 100 people in all age groups from 14 years and older. The proportion of men was 60% and women 40%. This allowed me to quickly obtain data from a broad audience in Switzerland.

To distinguish between experts and non-experts, I included a little logic in this survey to determine the way in which they would like to learn more about this technology. Of the 100 participants, 10% were experts and 90% non-experts. Of the eight total questions, the sixth and seventh questions were the most decisive.

The majority of the experts prefer to acquire more information in an interactive, explorative, experimental, playful way. The minority prefer a traditional informative way, including text, graphics, or animations. The non-experts preferred to deal with the topic in a combined (informative and interactive) way.

From this statement, I, therefore, decided to consider both in my work and to convey the technology of computer vision in the following manner: 3/4 interactively and 1/4 informatively.

Questions:
Q1: How well do you know about artificial in telligence (AI)?
Q2: Have you ever heard of computer vision (CV)?
Q3: Do you know how computer vision works?
Q4: What do you imagine by this term?
Q5: How did you acquire the knowledge?
Q6: In what way would you like to learn more about computer vision?
Q7: In which way would you like to learn more about computer vision?
Q8: At what level do you think it should be taught?

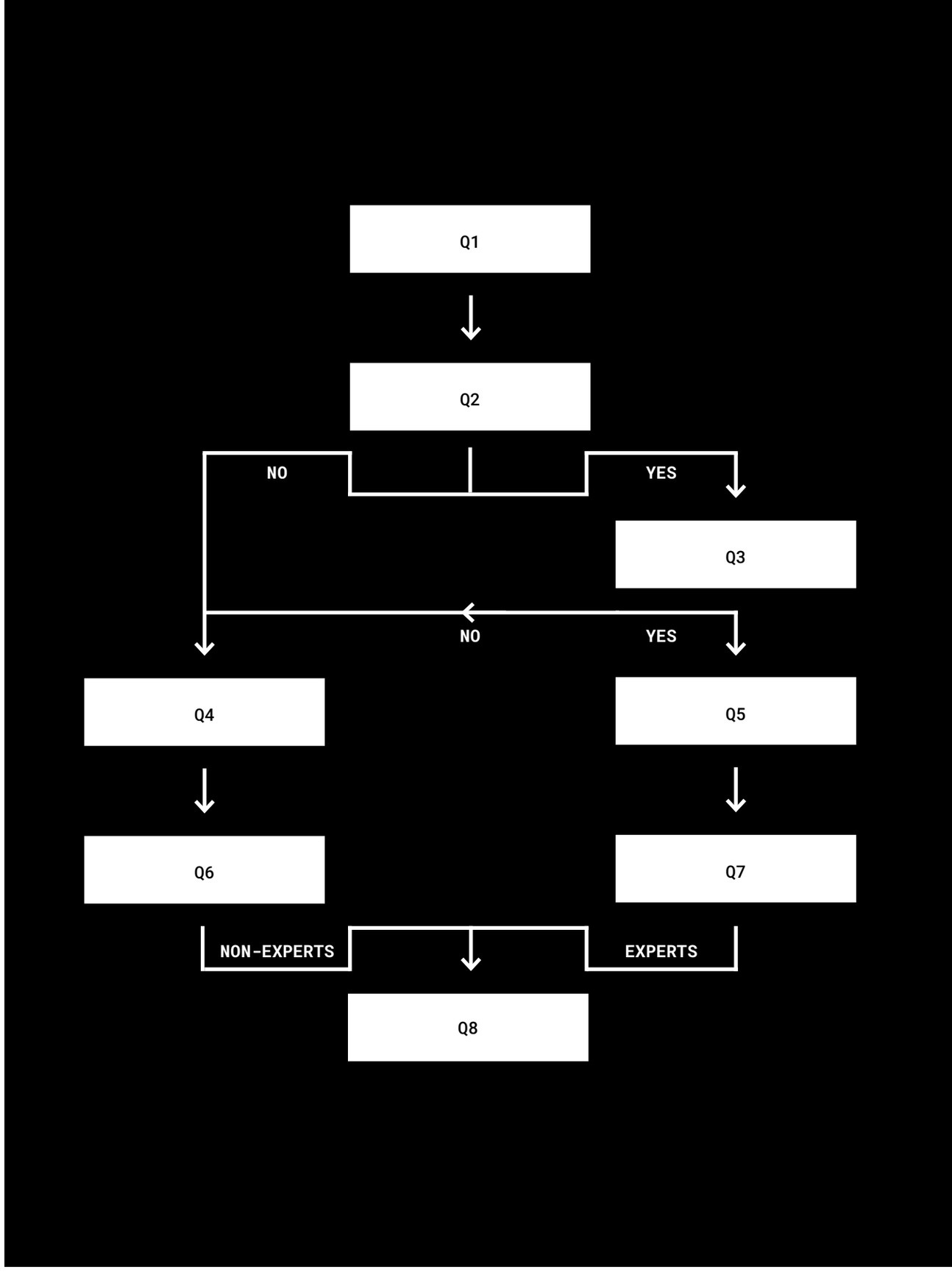

Figure 4. Survey Decision Tree (Source: Own representation)

CHAOS COMPUTER CLUB ZÜRICH (CCCZH)

The Chaos Computer Club Zurich (CCCZH) is a community where fun with computer devices play an important role without losing sight of the social aspect. It especially pays attention to the social effects of new technologies and aims to identify and critically evaluate tendencies by gathering experience at an early stage. They are interested in addressing the lack of transparency and limiting factors of computer devices, for example, to determine ourselves which data we wish to share and which we wish to access freely.

I originally planned to participate in a public Chaostreff, which takes place every Wednesday from 19:00 in the Hackerspace in the Zentralwäscherei Zurich. However, due to the current COVID-19 pandemic, it was not possible. For an alternative and uncomplicated contact, I used the internet relay chat (IRC) to spontaneously receive their thoughts about the development of biometric facial data. I also wanted to hear about the implications, opportunities, and risks of facial recognition technology.

A member named Cmdr_Zod answered my open questions and provided many valuable inputs. His real name is Peter Rohrer. He mentioned that one of the problems that technology has in common with fingerprints is the uniqueness of one's face. The problems are not identical. In the case of fingerprinting, there is a risk that someone might steal someone else's fingerprint and then breach insecure access systems. With facial recognition, the technology determines how well it is protected. In the past, a printed photo was sometimes enough. From his point of view, the recognisability is more problematic. Once someone has collected facial data on a large scale, it is possible to use this for tracking, which is difficult to resist if the cameras and the technology used to work reliably enough.

He also stated that it is exciting to see, from a legal point of view, the security of the proceedings. If an account is password-protected, and it is misused, then the user is accused of using a weak password or giving the password away.

I asked him casually which commercial application he thought was a risk in terms of facial data. Unfortunately, he did not know the market but he stated that charlatanism was widespread, such as automated partner selection based on biometric data, or fortune telling. He always regards it as dangerous when the data is evaluated without knowing how it is done and without being able to defend against the result. Many applications are, therefore, conceivable, even those that do not yet exist. He offered an example of Swisspass in a future scenario for automatic train travel, in which you no longer have to buy a ticket at a ticket machine or on a smartphone, as the cameras in the means of transport would be able to record when a passenger gets on and off the train. However, he describes a possible problem in obtaining facial data, which is similar to obtaining fingerprints. An attacker can use this to simulate the presence of another person in relation to another system.

Conclusively, he described his criteria as follows: 1. there is little transparency, 2. no possibility of objection arises, and 3. the life of individuals is influenced in a relevant way.

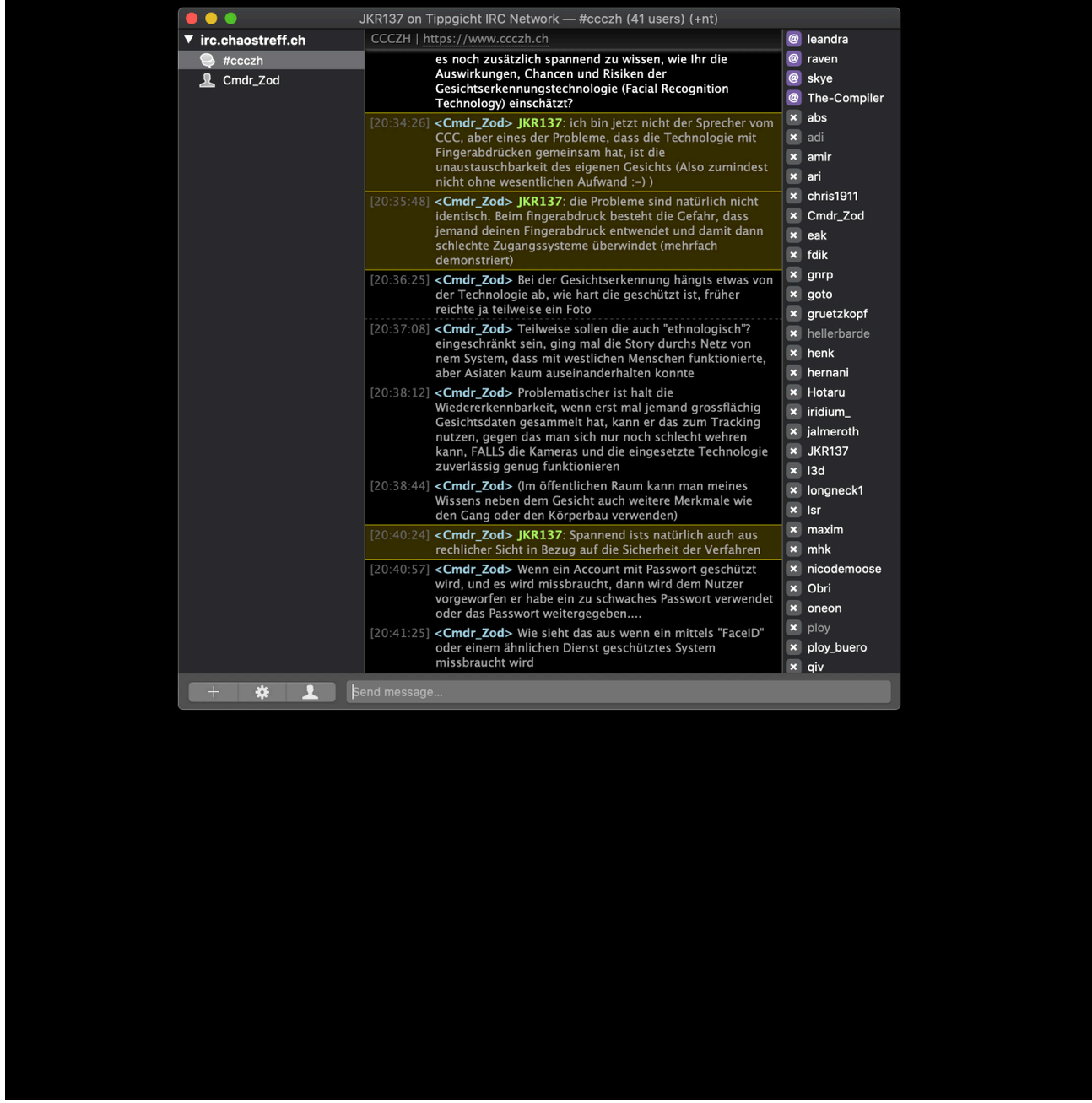

Figure 5. IRC Chat Window (Source: Own representation)

RELATED PROJECTS

CUBERA SOLUTIONS GMBH

To understand the perspective of pioneers that develop applications with face recognition technologies, I approached the company Cubera Solutions GmbH. The Swiss company recognized the potential of digital face recognition and, in 2017, launched its face recognition software called «Who is it?».

They also received an international media response with their innovative face recognition software on Microsoft HoloLens mixed-reality glasses. «Who is it?» recognizes previously saved faces in real-time and shows the wearer of the glasses all data known about the person. I would have had the possibility to test this personally, but due to the COVID-19 pandemic, it was unfortunately not possible.

According to Dominik Brumm (Head of Development), the benefits of this technology are far reaching and can be used in many different ways. For example, customers can benefit from a personalised service. This was tested in the first pilot project with the gastronomy company GLÜCK in Meilen to provide a better customer experience. The goal is to generate a positive experience for people who encounter their applications. For example, the customer's name, any allergies, the preference of a product can be entered and be available to the staff during the customer's next visit.

At the same time, the social aspects were addressed. Society often views the technology in a negative light, so the café attempted to show the visitors a positive aspect of permanent surveillance through this project.

Blattner added that there were, of course, other use cases, such as at an event, to identify the person addressed immediately and then exchange business cards digitally. At the same time, it is also possible to use it in medical applications to help people with memory difficulties to remember their loved ones. He mentioned that the specially developed software could thus be implemented in and adapted to practically any system.

The potential is significant and is already used by millions of people every day. Since the release of the iPhone X, unlocking the smartphone with the face has become a daily routine for many people. Therefore, social responsibility plays a decisive role in the company. Working with facial recognition and biometric data, in general, is a major responsibility for the company. Consequently, they often make a public appearance with «Who is it?» to raise awareness among consumers and decision-makers in companies. It is important to them that their technology is used in a responsible and data protection-friendly manner and that all personal rights of all those involved are respected.

It is encouraging to see that the company also considers the social aspects and closely examines the use of its face recognition technology. Nevertheless, consumers should be informed and have the right to refuse or agree to have their face features evaluated.

MEGAPIXELS

MegaPixels is an independent art and study publication that explores the ethics, origins, and personal privacy implications of facial recognition image-training datasets and their function in the advancement of biometric surveillance technologies. It aims to provide a critical perspective on machine image-training data sets that are often used without the explicit consent of the person they depict.

The creators, Adam Harvey and Jules LaPlace, launched this project in London in 2017 in collaboration with Tactical Technology Collective for The Glass Room exhibition.

Using facial recognition technology, the installation attempts to identify the user's identity in real-time within the largest publicly available facial recognition data set, known as MegaFace.

The five best matches are displayed on a screen with the purported confidence scores. If a similar face is found, a button lights up and you can print a summary of the result using a thermal printer based on information.

The visitors are not aware that they might be themselves in this dataset. The MegaFace dataset contains approximately 672'000 identities among these 4.2 million photos, which were obtained from the photo-sharing platform Flickr without any permission. Of the approximately 15'000 visitors, two people were found in this database without knowing that it existed.

Currently, MegaFace is used in academic, commercial, military, and government applications around the world to train and evaluate state-of-the-art face recognition algorithms. There you immediately ask the question of how you would react if your face, the face of a friend, or your child were used for the development of autonomous weapons – what objections would you have? Or how would you even find out if you are in this database?

This ongoing project has deeply inspired me because it allows me to investigate, experientially, the database that has been used to train face recognition algorithms without the consent of individuals. I identified a strong correlation to my aims. Similar to this project, I am attempting to make these critical sets of faces accessible and experiential to a broad audience in a provocative way, thereby exploring and questioning the ethical implications to stimulate discussion.

HAVE I BEEN PWNED? (HIBP)

In 2013, IT Security expert Troy Hunt created "Have I Been Pwned?". This website enables internet users to check whether data breaches have compromised their accounts. The service gathers and analyses hundreds of database dumps and pastes that contain information about billions of leaked accounts, and it enables users to search for their information by entering their username (usually their email address) or password. The platform has been widely regarded as a valuable tool for internet users who want to preserve their privacy and security, and this service is now used by Mozilla (Firefox Monitor) and the password manager 1Password to warn users if their login details have been compromised.

This website fascinated me mainly by its functionality, as I know how it feels to be a victim of a data breach and even to lose access to my account. Despite the numerous security precautions often the operator does not store the login data securely enough.

The user has to regain control over his data. All kinds of data can be valuable in some way because they can be sold profitably on the dark web.

However, I can change my mail address or my password at any time. With stolen biometric face data, the situation is different. If you lose them, you also lose a unique and personal data, which cannot be changed anymore. You can change something you know, but not something you are. This observation could be taken into account in my project, to highlight the problem.

URME

URME is an artist-driven and non-profit intervention that aims to protect the public from facial recognition surveillance systems by creating anti-surveillance devices. The artist and founder Leo Selvaggio considers identity in today's world to be highly manipulable, editable, and corruptible data. In 2013, he launched the URME Surveillance campaign on the crowdfunding platform, Indiegogo, using his own identity on devices as a decoy to fool the facial recognition systems in the public.

URME Surveillance currently consists of three primary devices. The first is the URME Prosthetic, which is a photorealistic 3-D printed mask of the artist's face. The second is an economical alternative for groups of activists named URME Paper Mask, and finally the URME Facial Video Encryptor, a specially developed software that encrypts the user's face by digitally replacing it with Leo Selvaggio's face.

When people use these anti-surveillance devices, camera systems equipped with facial recognition software identify the user as Leo Selvaggio. In this way, the wearers of these devices protect their own identity by exercising their persona in the monitored areas.

I view this as a courageous and successful approach to "sacrifice" one's own face to protect the faces of others against these widely used facial recognition technology.

This movement against surveillance fascinates me, as these devices are used to trick other devices in return. This is also an interesting way of exposing the risks of biometric facial data and making them accessible to a wider audience in a critical way.

CV DAZZLE

CV Dazzle by Adam Harvey, similar to URME, is a response to the increasing surveillance of society. He explores how makeup and hairstyling can be used to dazzle facial detection and recognition systems by altering the contrast and spatial relationship of key facial features. The name comes from a type of World War I marine camouflage called Dazzle, which used cubist-inspired designs to break the visual continuity of a battleship to conceal its orientation and size (Harvey, n.d.).

It is remarkable how an old design pattern from the WWI era has been revived to avoid detection by current computer vision technologies and how these facial detection algorithms can be dazzled with simple methods. Therefore, the simplest implementations of ideas are often the most comprehensible. This is something I keep in mind.

GOOGLE ARTS & CULTURE APP

In 2018, hype emerged about the app from Google called Arts & Culture because of the Art Selfie function that allows you to discover art playfully. As soon as you take a selfie with the app, it creates a faceprint using facial recognition technology. Each selfie you upload is compared to the database of available artwork to find the doppelgänger.

This means that to find an art twin with "Art Selfie", a portrait photo must be uploaded to Google's server each time. This has been criticized because these selfies could use Google to train its recognition algorithms.

Google's terms of service (January 22, 2019) state the following:

> When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services.

This is critical and the users of such apps are not adequately informed about what happens to their faceprints. I attempt to investigate this problem further in my project.

ZOOM PAVILION

Zoom Pavilion is a panoptic audio-visual installation from the artists Rafael Lozano-Hemmer and Krzysztof Wodiczko that was exhibited firstly in 2015.

It features 12 computerized surveillance cameras trained on the public with an immersive projection mapping in a room that visualises this ubiquitous predatory technology of tracking and control. Face recognition algorithms are used to detect and record each person's presence within the exhibition space. This should make the data-gathering mechanisms accessible to the audience in a playful way.

The installation does not attempt to identify individual persons, but rather monitors and records assemblies of people, as proximity is considered suspicious, thus allowing potentially secret and dangerous communication. Therefore, the state of the camera movements is fluid and constantly zooms in on various groups of people.

Because of this work, I think invisible surveillance technology is being made visible. Many of us already know that this technology exists and is being used, but I believe by experiencing such technology, opens up new ways of questioning this development and its power more critically. I do believe with this piece of work the technology loses some of its power, and we gain that power ourselves. I am convinced this interactive installation has shifted the balance of power of knowledge in the eyes of the people. Facing the power of these systems can have a significant effect and with my work, I attempt to address this approach.

CONCEPT AND ANGLE

Based on the research part I analysed different applications in the field of computer vision. I divided the applications into two main categories: commercial applications and industrial, advanced applications. I noticed that facial recognition technology is actively and passively represented in almost all applications of computer vision. This surprised me personally that the use of this technology is not limited to just unlocking a personal device or the use of surveillance cameras. I was astonished that in further research and discussions with experts I came across numerous areas of application of facial recognition technologies, including those that are conceivable in the near future.

This led me to examine the disadvantages, problems, risks, advantages, and opportunities. As a result, I was able to conclude that the risks outweigh the opportunities. Furthermore, commercial interest and investment are continuously increasing as technology becomes cheaper and more accurate. It is also becoming increasingly common. In turn, convenience and simplicity are seen as beneficial by consumers, as there are fewer touchpoints for the same purpose. It improves the user experience and this trend drives the mass adoption of face recognition in commercial applications.

Due to the poor and incomplete regulations regarding the use and processing of biometric facial data, the regulatory authorities are not catching up fast enough. As a result, there is no uniform framework for their use and their limits. Some private individuals and smaller companies take advantage of the situation to obtain these facial data in secrecy, both legally and illegally, to generate high profits.

A photo of a person is no longer just a photo. It is a defining feature of an identity that could be used, shared, or sold in ways that consumers do not understand, anticipate, or consent to. In serious cases, it can be used to train ethically questionable technologies. Once the biometric data is compromised, it affects all applications at once for the rest of the person's life.

Therefore, my goal is to communicate the vulnerability of biometric facial data to a broader audience to deal with the topic experientially. In this way, I attempt to create awareness and stimulate discussion and scepticism about the legal position of facial recognition technologies at the current state. As with fingerprints or ID cards, they cannot simply be collected and disseminated by anyone. This should also apply to biometric facial data.

Many applications often attract consumers with free services to get their facial data in a legal and "cheap" way. The privacy statements are usually written in such an encrypted way that it is not understandable for laypersons and so that it does not sound negative, to avoid deterring consumers if they do read it. This gives companies and individuals the power to do whatever they want with these facial data.

The problem with this kind of personal data is that it is an abstract and intangible construct, in that it is very difficult to understand what exactly happens to this data. Several approaches address facial data and its risks. In my work, I attempt to make the abstract and complex topic tangible, to question the ethical effects of face recognition technology on daily life. One underestimates the risks, although there is some awareness that personal data are stored and used on a large scale in a certain way. My challenge is to create an effective and provocative level that captures the user in this experience, thus allowing them to reflect and sharpen their awareness.

Therefore, I could imagine designing a kind of interactive and bold prevention platform. A critical design approach is also possible, which could be much simpler and more impactful. For a critical design to be successful, users should be able to form their own opinion about the current situation and possible future. It would be interesting to position them in an ethical-moral decision situation, and designing an effective measure to counteract this trend and, thereby, mitigate harmful consequences or undesirable situations.

FINDINGS AND NEXT STEPS

While researching, I noticed that many terms in the area of my topic are often used interchangeably. I took note of this, as it is an important factor to avoid confusion and not to rely on false information and then convey it later. Of course, I was aware from the beginning that my topic is complex and expertise plays a key role. Therefore, I spent an enormous amount of time to gain a decisive overview of face recognition technology, both theoretically and practically. This allowed me to acquire basic knowledge, and I found that I was able to move more confidently in this topic, which I started to value.

After the second progress session presentation of my BA thesis, I received feedback stating that I should be more specific as it was not yet clear in which direction it would exactly go. Furthermore, I should always keep the contribution in mind along with my work.

The initial idea with the first web application click dummy prototype (see Prototypes on page 56) was to show the user's side as well as the other side, how things happen behind the scenes in the many applications. The idea was that the user could control an avatar in real-time with his or her face and switch to "transparency mode" with the help of a toggle to convey the risks of facial data experientially. During the mentoring, it turned out that I should encourage the audience to use the avatar more, be more captivated by the experience, and be even more provocative.

My next steps are to test ideas using prototypes with the involvement of people and get their opinions so that I can build on them and be involved in the design process. Thus, I will personally look very closely at the possibility of implementation in order not to jeopardise the timetable and the criteria. To adapt to the current situation (the COVID-19 crisis), I decided to develop a web application. Based my experiences during my studies, I was able to apply decisive insight. Before I start with the implementation, I will create prototypes with the tool Figma and have them tested and evaluated by people. This also helps the implementation, because, according to my experience, it saves me from having to do it several times and, therefore, I could remain efficient.

III

PROJECT DEVELOPMENT

INITIAL IDEA

PRETOTYPE V1

In the BA Thesis concept seminar, we explored our interest to develop a concept, which we had to present it understandably and visually. As I was fascinated by some of the topics, I took the time to take a closer look at them. I was very interested in the interaction between a computer and a human being because I always asked myself the question, how the view of a computer looks like.

For the pretotype, I quickly and efficiently generated a 3-D rendering with the program Blender, which helped me to better visualize the immersive virtual environment. It also allowed me to explain my first idea to people in a more understandable way. The idea was to create a virtual environment with a production line and objects on it, in which the person wearing the VR headset has to process the task by sorting out two differently marked objects correctly to ensure that the second person on the computer can use it without interference. Furthermore, the person in the immersive virtual environment could even see its operator in real-time to perhaps see its reaction based on the decisions and actions.

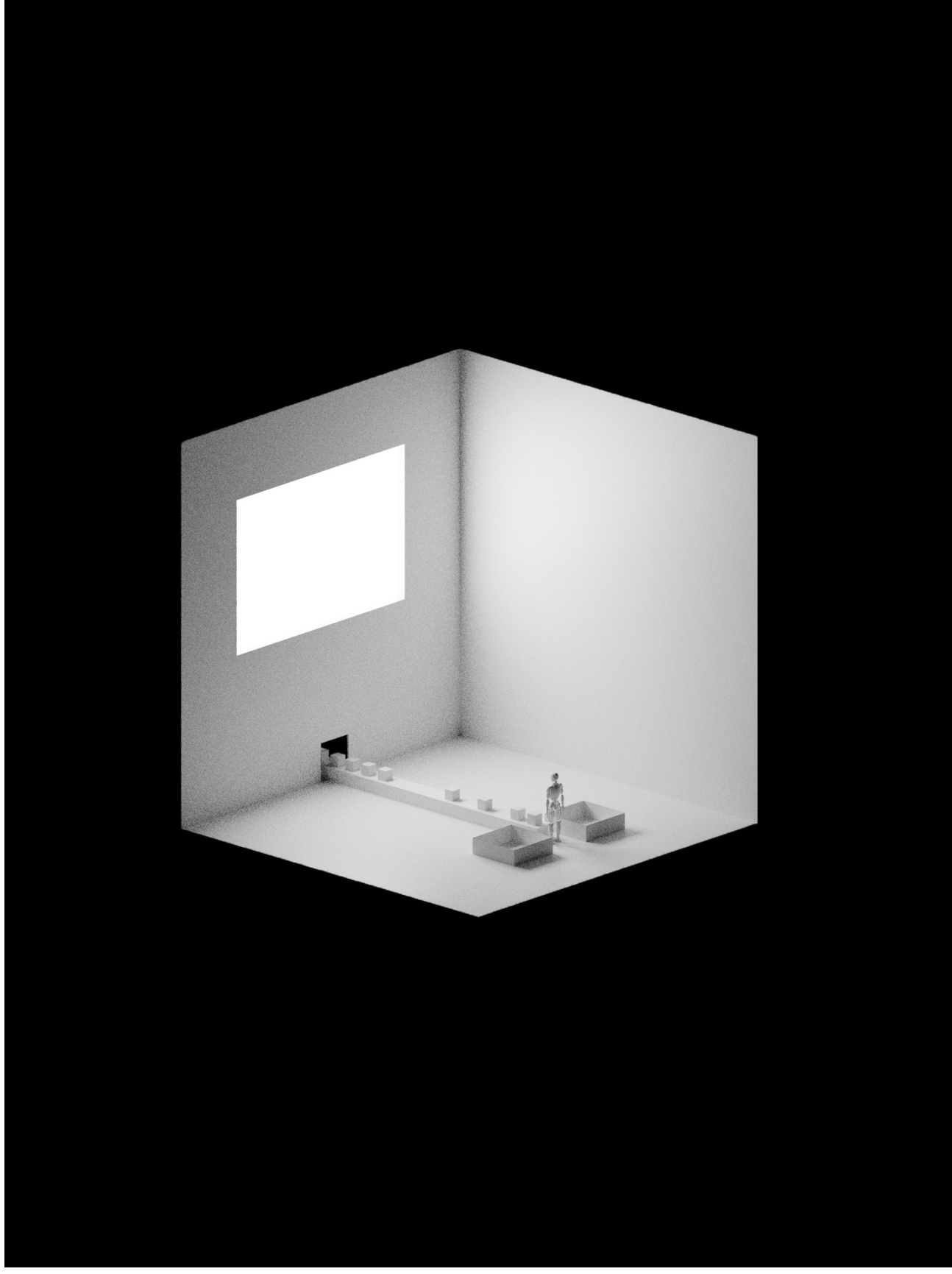

Figure 6. Pretotype V1 Rendering (Source: Own representation)

PRETOTYPE V2

After some feedback and iterations from the first pretotype, I started to design the immersive virtual world with Unity. I wanted to have my initial idea not only visually in front of me, but also to dive into it. What I planned to investigate at this point was the interaction between a computer with a mind and its operator. The idea was that the person or the “living operating system” in the VR environment could help or even annoy his operator, for example by panning the menu window back and forth or deleting a file without being asked.

I used VR as a medium because it can create a level of empathy and understanding that is often more effective than any other form of communication. The reason for my project was that because artificial intelligence is one of the fastest developing areas of human technology, it is important to understand our relationship with it, and it would not hurt to start thinking about the possible implications for ourselves and especially for future generations.

After the first progress session presentation and mentoring, however, it turned out that my project is very elusive and lies too far in the future and, therefore, had a little factual basis.

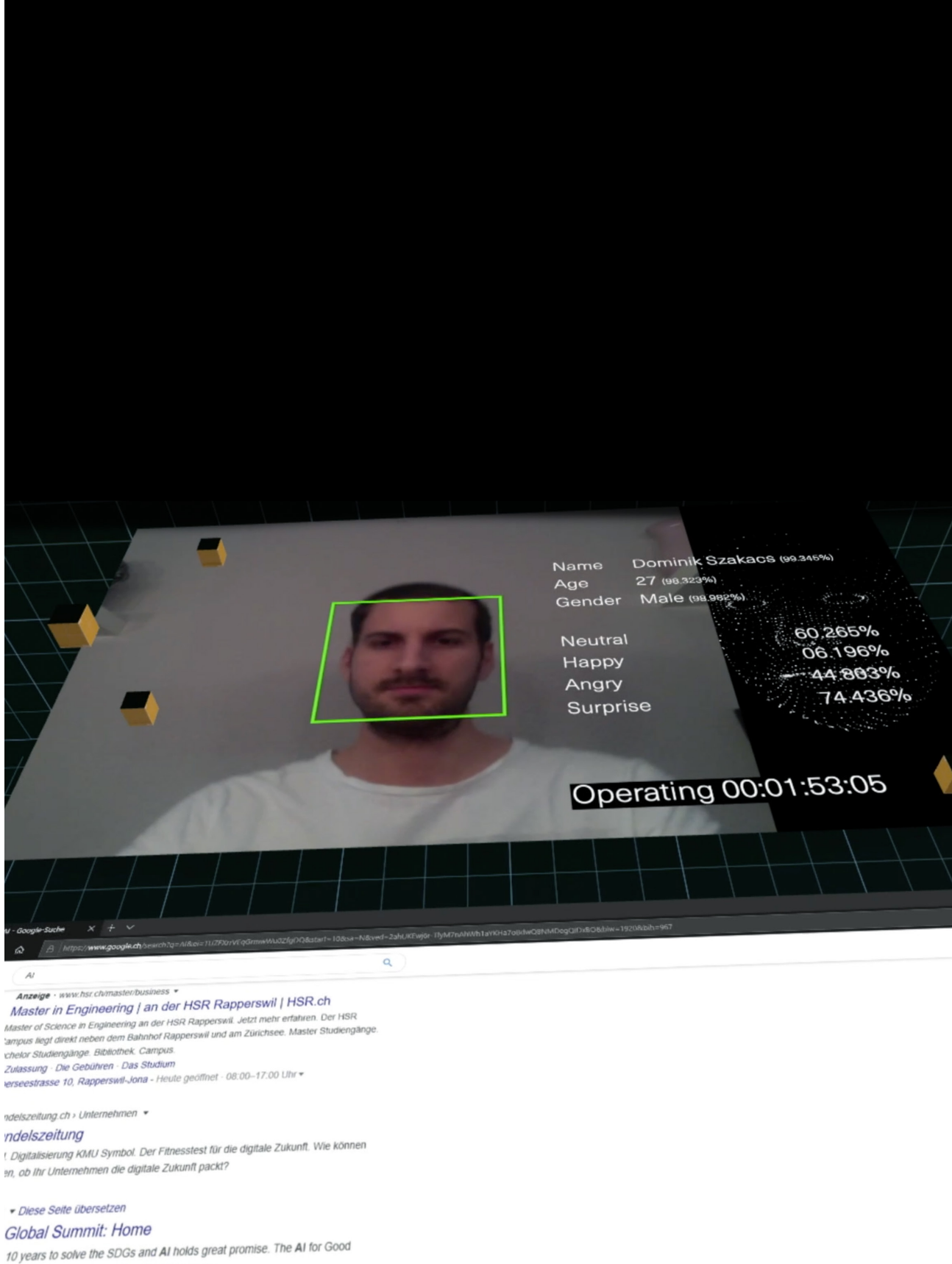

Figure 7. Pretotype V2 VR (Source: Own representation)

TOPIC DEVELOPMENT

Therefore, I took a few steps back and came across the following quote from Fei-Fei Li, a well-known person in the field of computer vision: *"If we want machines to think, we need to teach them to see".* Therefore, I invested a great deal of time in the topic of computer vision to immerse myself in it, which should give me a decisive overview. I was interested in virtual reality even before I started working on my BA thesis and I think it is important to build up not only practical knowledge but also theoretical knowledge. Therefore, computer vision was an ideal topic, as it allowed me to gain some additional understanding of how modern VR and upcoming AR glasses with tracking cameras work, as well as other applications that surround us every day.

Through research, conversations with people, and experiments, I tried to come across a problem that I could use to convey in an experiential, interactive way to a wider audience. Over time, I narrowed down the broad theme of computer vision and focused on facial recognition technology. It turned out that a certain awareness already exists in this area, but the potential risks cannot be assessed at all. This also encouraged me to investigate this more closely and I was surprised to see how many applications with facial recognition technology are already in use. Especially the excessive use of our face in more and more consumer applications is something I have questioned and has opened up my eyes. This led me to the biometric facial data, which is increasingly being used in the consumer sector.

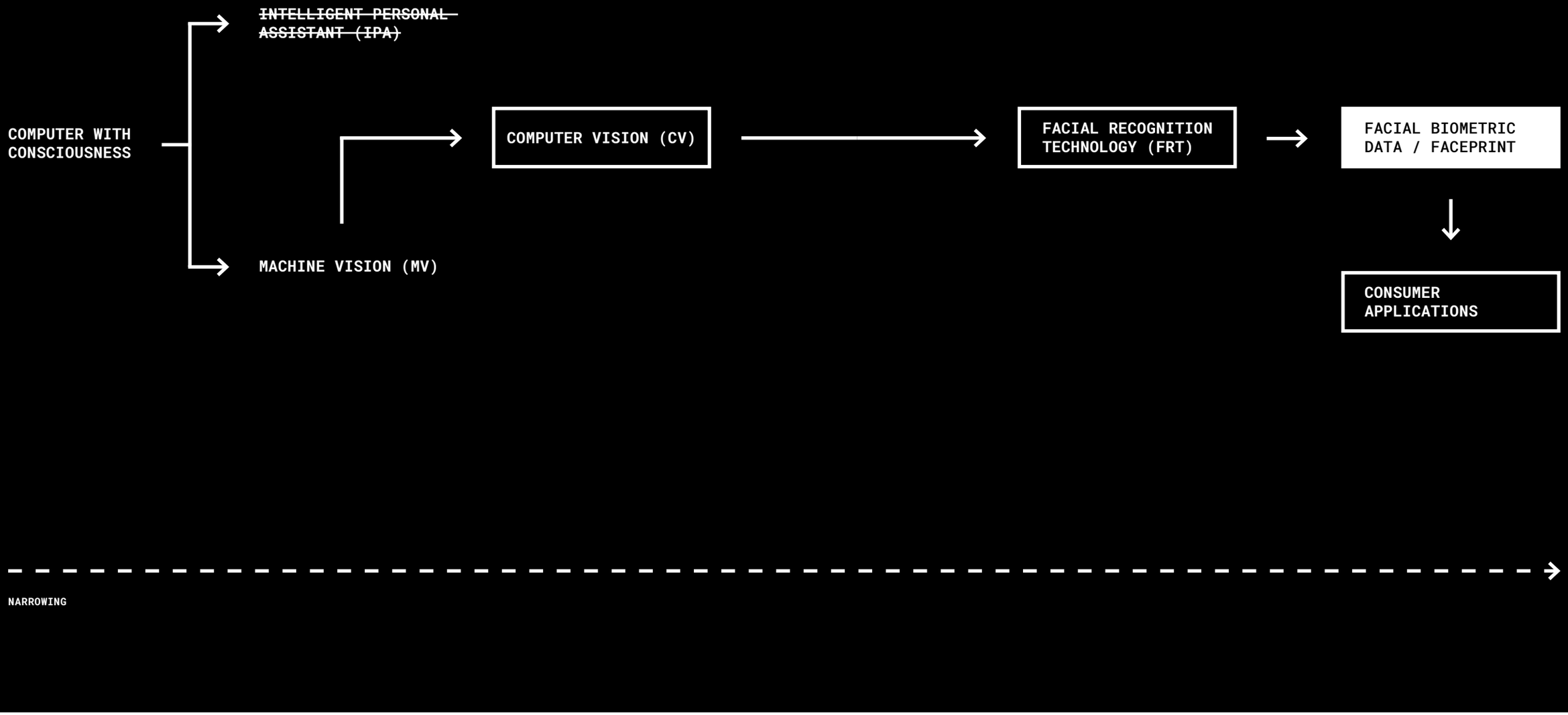

Figure 8. Topic Development Branch (Source: Own representation)

EXPERIMENTS

HUMAN ARRAY EXPERIMENT

During the research and even in the concept phase, I had struggled with what to do next. In order not to lose myself completely in reading, I decided to experiment without much hesitation. I asked myself the question of how it would feel, as a human, and how the result would look like to perform a classical and simple task of a machine. The task was to interpret and approximate an image from the perspective of a machine.

I attempted to take a very simplified and grayscale picture. Converted, it consisted of 12 columns and 16 rows, each with an 8-bit number, whose range is from 0 (black) to 255 (white) and, therefore, represents the brightness. This resulted in 192 input values I filled in the grayscale values using a pencil and pressure ratio manually for each pixel.

It was surprising to me that I started with the lowest number first, instead of the first in the order, as is normally done by a computer. To match the grey-scale values, I worked from the inside out but had to make many corrections because it was often not consistent with the same or the nearest number. The result was quite surprising and I never thought it would work so well. Moreover, computers can do this within fractions of a second compared to the 45 minutes that the same task took me to do.

This experience inspired me to convey the foundation of computer vision simply. I took the so-called MNIST database as an example. It is a large database of handwritten numbers from zero - 9, which is mentioned and explained in several books in the field of computer vision. I wanted to bring this to people with little or no knowledge by creating an interactive installation.

The idea was to take up the black box problem and show the users what is happening behind this seemingly simple input and output.

With the help of feedbacks in the mentoring sessions, I decided to focus more specifically on an application that might be more interesting for an audience. I also decided to keep the technical aspect more in the background and put a stronger emphasis on the implications of this technology.

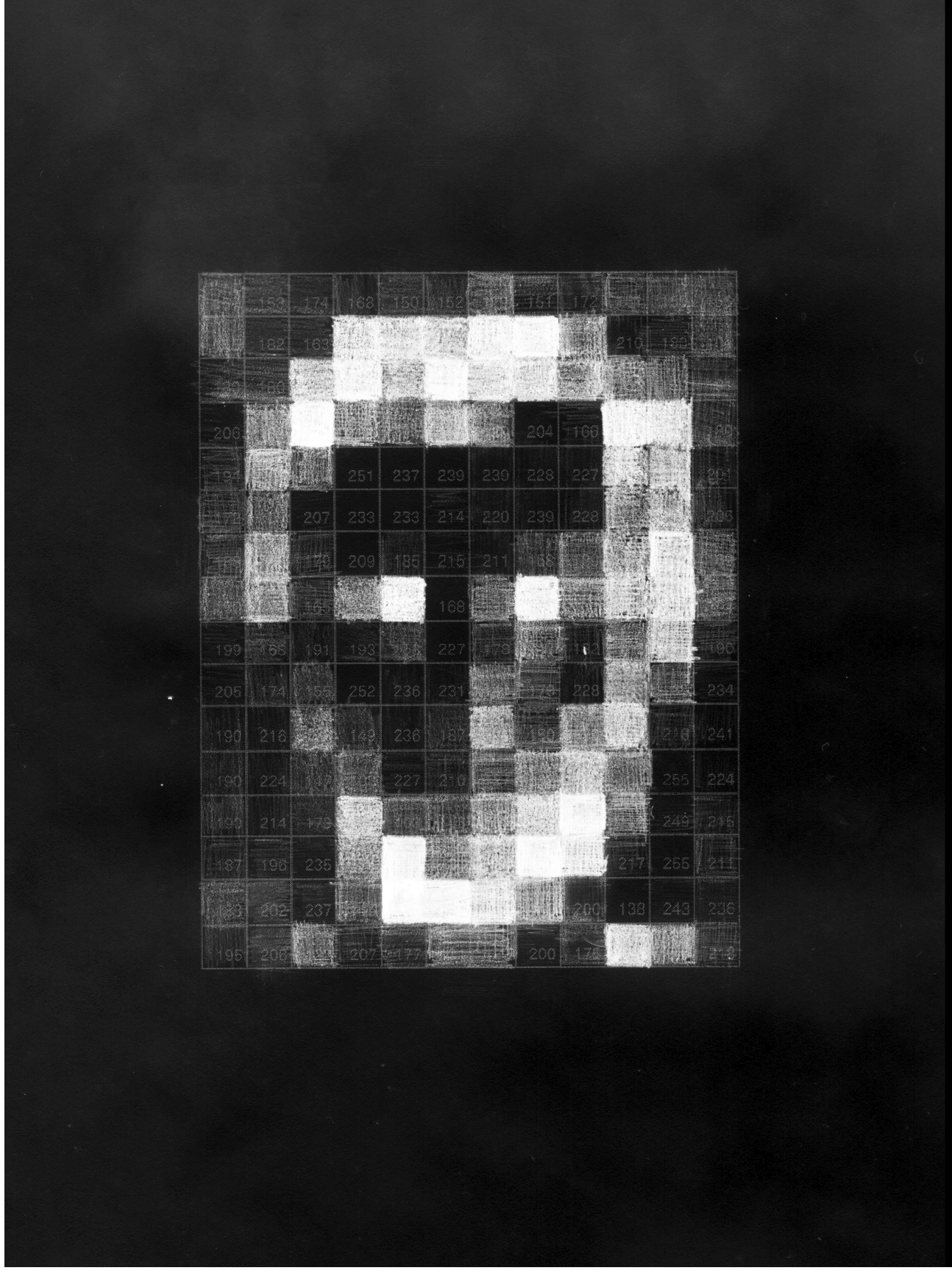

Figure 9. Human Array Experiment on Paper in Negative (Source: Own representation)

MR FACE EXPERIMENT

Based on the findings from the earlier experiments, I built a Mixed Reality Face Detection Device using Unity including libraries, Android mobile phone, and VR Cardboard glasses. With this experiment, I tried to take the view of a face detection algorithm, that operates in real-time. An idea came up that the person with this device would be able to train the algorithm in real-time by looking at different faces to identify human faces around him/her.

The implementation of this experiment took quite a long time and was partly overstrained due to the libraries and the many compatibility conflicts. Furthermore, the COVID-19 pandemic was a complicating factor and I had to adapt the concept once again so that the audience would still have the opportunity to engage with my work, even from their home. This required a rapid reaction and I rejected the idea and continued to work out additional concepts.

Figure 10. MR Face Experiment with VR Cardboard (Source: Own representation)

PROTOTYPES

PROTOTYPE V0

Unlike facial detection, facial recognition additionally analyses the unique structure of the face and converts it into code and this code is called facial biometric data or faceprint and is then compared with a database until a match is found. The match is often returned with attached information. In my prototype with facial recognition, I was able to display the name of the person that was recognized, as well as having a bounding box around the face.

I tried out several instructions from books, videos, and blogs and, as a beginner, I was often overwhelmed, because despite the acquisition of knowledge through research in a short time window was not enough. Fortunately, I found the PyImageSearch community website after some time, which allows me to do a small project in the field of computer vision and deep learning without having to deal with mathematics and theory for a decade. From the beginning, it was important to me not only to work through a list systematically, without knowing why I am doing it, but also to determine the reason and thus acquire the knowledge sustainably.

To get started, the free program library with algorithms for image processing and machine vision called OpenCV is recommended. The installation was a challenge because it required the terminal. I, therefore, used the pip (Python's package manager) installation method to install OpenCV on the system and configured the development environment. I also used a client-server application called Jupyter because it allowed me to run scripts in real time. It is also widely recommended.

To interfere with OpenCV's face detection algorithm, as a side experiment I formed some shapes with black adhesive tape, which I stuck on my face. The inverted T shape on the bridge of my nose worked best and it was amazing to discover that it also did not work with FaceID on the iPhone.

After the second Progress Session presentation, I received the feedback that I had to be more specific, as it was not yet clear in which direction I would go. Furthermore, I should always keep the intended contribution in mind.

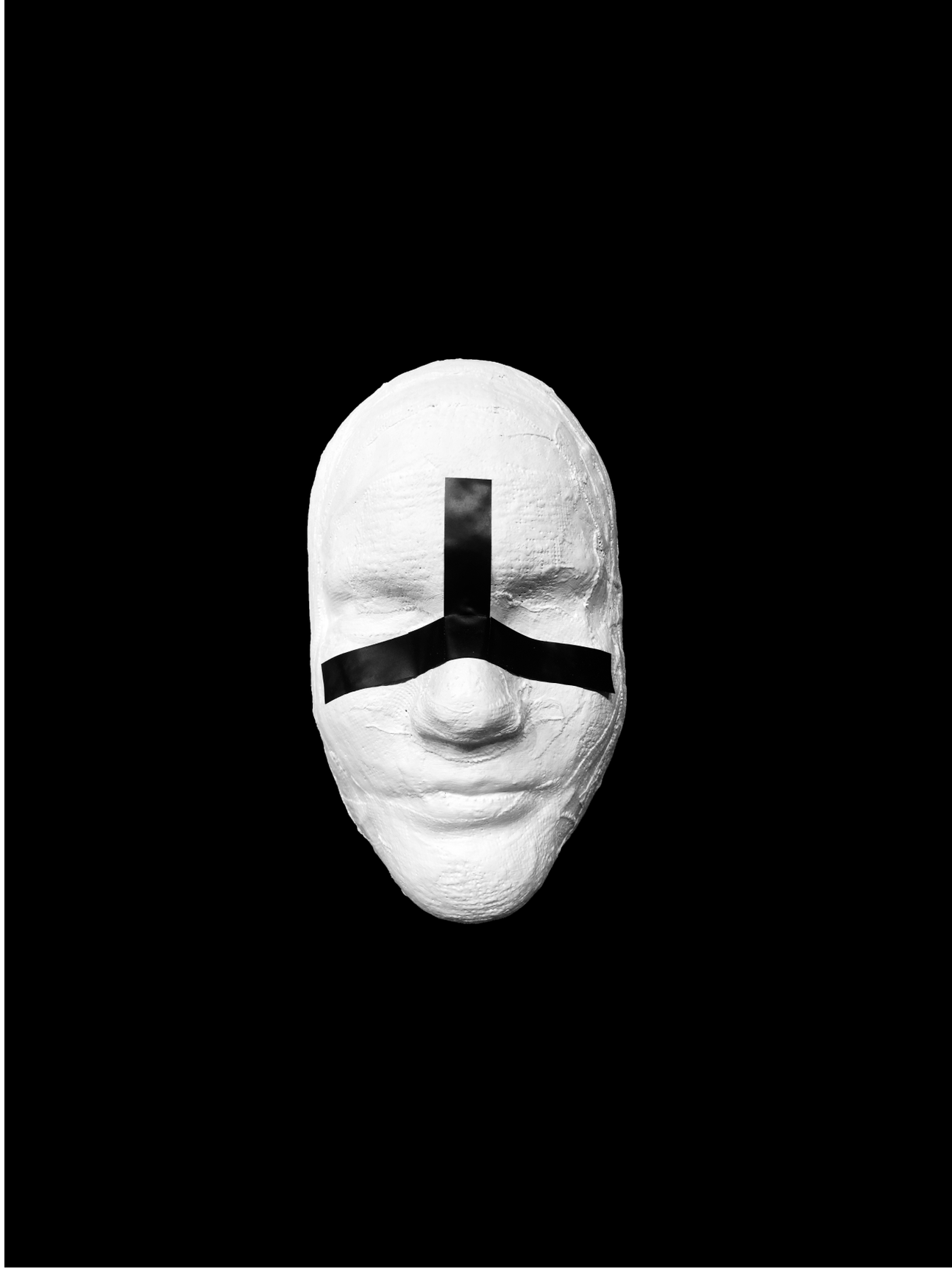

Figure 11. Prototype V0 for Jamming OpenCV Face Detection Algorithm (Source: Own representation)

PROTOTYPE V1

After the feedback from the lecturers, I investigated the applications in the consumer area even more closely. Thus, I discovered interesting paragraphs in the privacy policies that shocked me and, at the same time, fascinated me because I saw how cleverly some of the sentences were formulated.

> *We may use and share non-personal information (meaning information that, by itself, does not identify who you are such as device information, general demographics, general behavioral data, geolocation in de-identified form), as well as personal information in hashed, non-human readable form (Tinder, 2020).*

> *Ever uses facial recognition technologies as part of the Service. Your Files may be used to help improve and train our products and these technologies (Paravision, 2020).*

The majority can imagine very little of it. Evidence suggests that facial data is likely to be used and shared in the form of code. Since on dating platforms much personal information is often disclosed, the connection with facial data can be quite interesting for the development of future applications.

As a result, I decided to design a web application that would demonstrate this problem to the user in a very unexpected way. Using Figma, I created a click dummy prototype by showing the user's point of view as well as the other side, how things work behind the scenes in the many applications. With the help of a slider in the menu bar, users could switch between these two sides in this prototype. To visually distinguish the two pages, I selected a strong contrast. The light side represents an everyday user who is able to control an avatar in this prototype with the help of the webcam and could switch to the dark side at any time by being confronted with the collecting mania of the face data in the background.

Discussions with my mentors indicated that it is not sufficient to control only a virtual avatar. It appeared to be not riveting enough. Therefore, I took the concept further to encourage people to use the application even more while keeping them engaged in the experience.

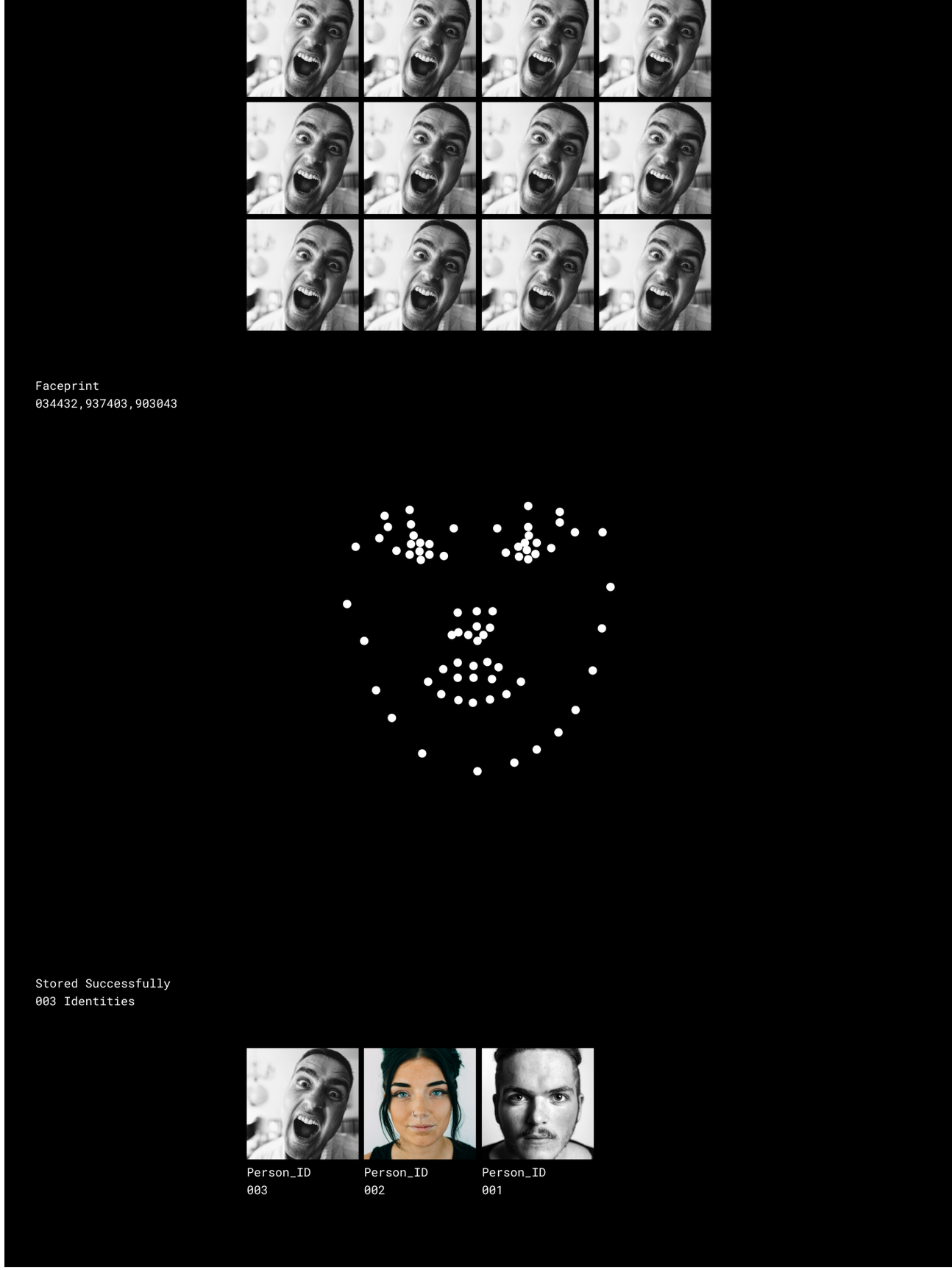

Figure 12. Prototype V1 (Source: Own representation)

PROTOTYPE V2

Thereafter, I attempted to refine the communication strategy and approach it from a teaching perspective, providing the user a lesson or throwing them into the deep end to create a more conscious behaviour with real applications. In other words, I aimed to identify the risks of biometric facial data concerning commercial applications and to advise them on how to protect themselves from them.

Therefore, the second click dummy prototype was geared to prevention. The goal was to address the risks of common apps with camera access or access to private photos with faces.

To encourage people to use the web application more, I drafted a banal application that promised you can release neck tension in a playful approach with the help of face tracking. However, in the background, app stores facial images in a database, as in the initial prototype. The therapy game was ideal because you can capture the face from all sides. The idea of the game was to move a point that you can control with your nose into the given squares as quickly as possible.

Before being able to use it, however, users had to accept the terms of use and privacy policy. In contrast, I have adapted the privacy policy in a way that allows with the given consent of the user to use their facial data to train facial recognition technologies.

The users had to decide after the therapy game in which facial training category their face data should be used. The purpose was to put the user in a shocking moment and see for themselves that they had agreed to something they would never have done if they had read it carefully.

During the tests, though, it was discovered that the test subjects found it difficult to understand and, therefore, far too complex and confusing. I lured them more in one direction only and through these tests and discussions, it was clear that it was also going in the direction of deliberate deception and was not considered effective. Often I was asked whether it was mainly about the privacy policy or the therapy method.

I then had to create something far more effective and simple by focusing on the facial data again.

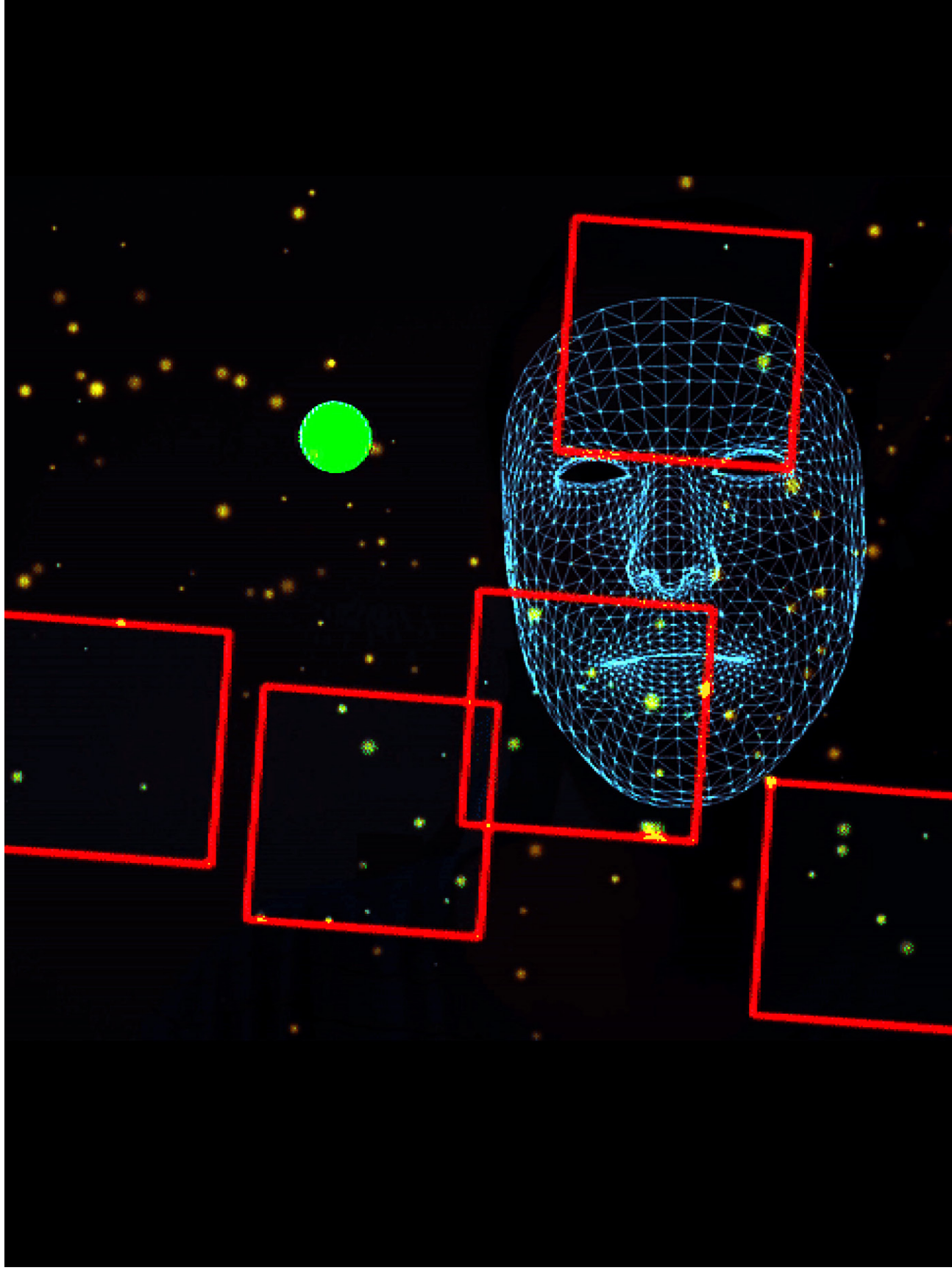

Figure 13. Prototype V2 (Source: Own representation)

PROTOTYPE V3

I took some time to clear my head and came to a crucial realization that a simple photo of a person is no longer just a photo, but it is rather a defining characteristic of identity. This identity, for example, can be taken without the knowledge and consent of the person concerned, and it could be used as training data for unethical, questionable technologies or just be passed on.

The excessive uploading and downloading of facial photos change the meaning of the human face enormously. The more our face gets onto the internet, the more we lose our identity.

The situation is similar to gambling. The more often you place money, the more likely you are to lose it again. I attempted to incorporate this analogy and created the third concept on a prototype. I decided to use a very simple game. The slot machine is an ideal choice because it animates the users to use the web application and it captivates them in the experience and most of it is already known. Unlike in everyday applications, where photos of people are shared and stored in their database, I try to give the chance to get those face photos back. I also considered the degree of difficulty for the implementation, which fortunately was considered feasible.

Like every technology, there is a bright and a dark side. Therefore, facial recognition technology also brings with it useful good intentions or opportunities, not just dangers. Unlike the other two prototypes, my goal was not to direct the users in a direction I determine myself but to allow them make their own decisions – to present a situation where the possible return is of secondary importance to the win of facial images.

With the help of the developed prototype, I explained to the user more clearly what my work is about. However, I had received feedback that without the explanation they did not know why it was about face photos at all. Therefore, I implemented an Onboarding screen in this prototype, which contains a very short written explanation, as well as a self-made video about my intention.

This time I received more positive feedback than previously. While it may be abstract, it is still understandable because it stimulates you to reflect on this topic. During the implementation, I involved the people more in the process and continually adapted the prototype based on feedback and concerns.

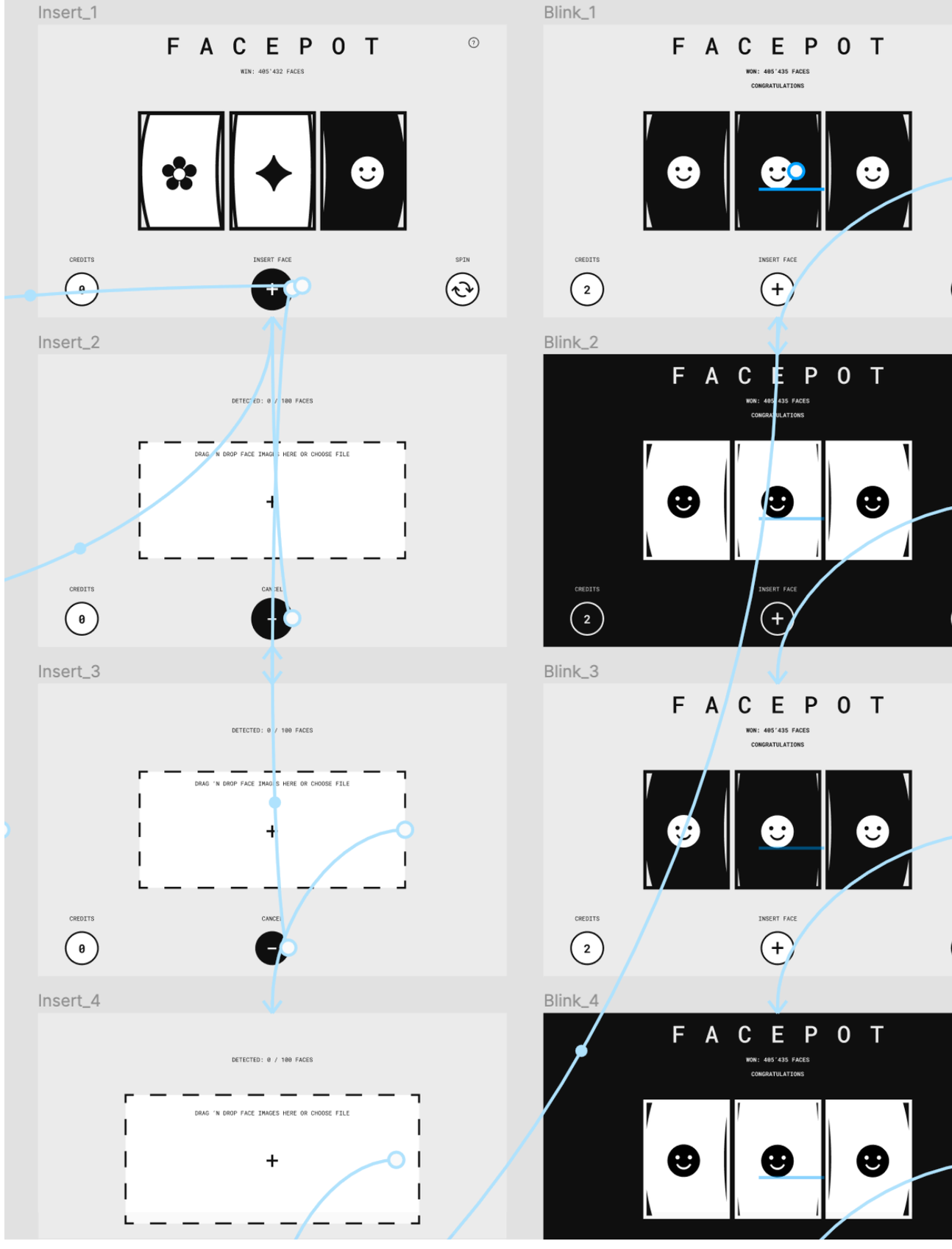

Figure 14. Prototype V3 (Source: Own representation)

VIDEO

This year, the visual presentation of our diploma thesis is especially important. Since a video was ideal for me to use on the landing page of my web application, I decided to set the video length to a maximum of one minute. My goal of the video is to effectively convey the context and the possible experiences with the web application and, at the same time, make them curious to use it.

At the beginning of the video, I briefly present the scientific context of my work so that a connection to the web application can be established. Without this, it turned out that many questions were generated. It was important to me not to explain the whole research field of face recognition technology. During the first storyboard, people already have a certain awareness. That is why I am going to focus on the project. One quarter of the video consists of an introduction and three quarters addresses the web application.

I mention that one has the opportunity to gain the power of decision over the facial images and to question the true value of this data. Furthermore, I show that they are confronted with an ethical and moral decision, whether they put their own face or that of another person at risk, to win back numerous new facial images in return. I raise the question of which side they choose and encourage them to reflect on whether they support or oppose this trend. The decision remains entirely up to them. They can use my web application and, at the same time, address the issue and critically question the way they handle this sensitive data in everyday life. Finally, I point them to the website.

For the visual appearance, I decided to use an animated video, which is strongly oriented on the web application. To work more efficiently, I decided to draw the plot of the video including a short description. So that I do not have to play every single animation in my head and thus relieve my work, I used Figma and quickly created a template with all transitions and animations. This helped me to coordinate the tempo with the voiceover and to make changes quickly. For the final realization, I used the program Adobe Animate to refine everything.

My challenge was to make the transitions and animations as dynamic as possible so that it did not seem too lifeless and, therefore, static.

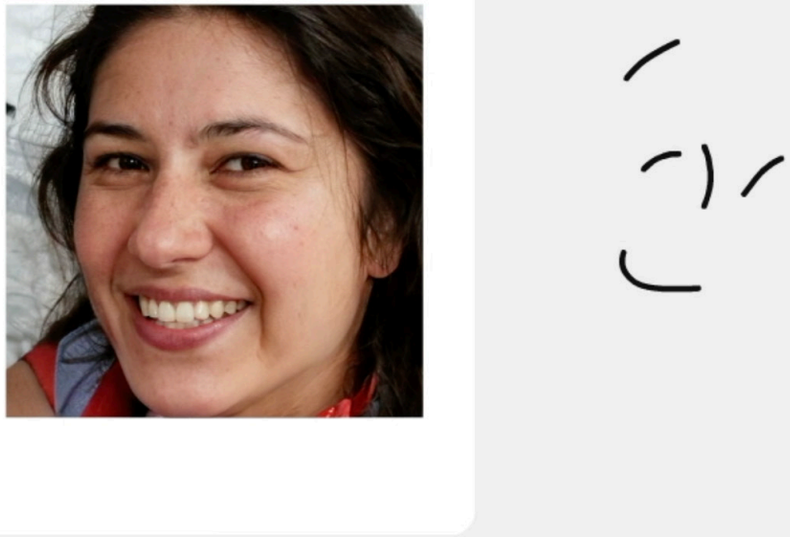

Figure 15. FACEPOT Video Screenshot (Source: Own representation)

RESULTS AND EVALUATION

INTRODUCTION

After evaluating the prototype, I decided to develop the Prototype V3 further. Therefore, the web application went in the direction of critical design. I checked the possibility for the implementation very carefully to keep the schedule as well as not to endanger the criteria. I immediately started to work out the idea with Figma and continuously tested and evaluated it with people.

VISUAL AESTHETICS

In terms of the visual aesthetics of the web application, I tried to keep it as minimalist and neutral as possible. A grid helped me especially with the placement and size of the objects. For the background, I used a greyish white, which is assumed softer for the eyes than true white. The whole website contains a palette of the following three hex colours: #EEEEEEEE, #111111, and #FF0000. A colour combination where the goal is to make clues stand out with gaudy eye-catching colours. The bright red only appears when the user presses the “Spin button” while the credit balance is at zero. The credit display lights up for two seconds and then goes out again. During the click dummy tests, people understood it immediately. The short flashing, as well as the colour red, was associated as something negative and, therefore, something must be done about it. It points directly to the problem that the credits should be topped up to use the slot machine. It is fascinating for me to see that small details like this kind of feedback can have a significant impact on the user experience. Out of curiosity, I set the “Insert Face/s button” to blink instead of the credit display. It directly indicates that the user has to click on the button, but you did not immediately know why.

Concerning the layout, I divided it into three main areas to allow an easy overview: at the top the menu navigation, in the middle the core element, and below the core element navigation. These main areas can be found throughout the other pages, where their position and size remain unchanged, thus ensuring consistency. I tried to create a sense of familiarity for the user on each page.

The three core elements of navigation symbolize the interactive possibility using the outlined design without filling. As soon as you move the mouse over it, it will be filled in, indicating that it is clickable. There is one exception, however, and that is the credits display, which looks like a button but does not react when you move the cursor over it. Therefore, I found a good balance between usability and aesthetics. I rejected the idea of zooming on the interactive elements while moving over with the cursor, because it does not bring any benefit and disturbs the visual appearance in my opinion, and interacting with the core element in the middle was too much of a good thing. The users, on the other hand, did not mention or criticize this in the tests. I reduced the number of buttons to a maximum of three by also taking into account the placement of the respective buttons. If the user wanted to continue or confirm his/her selection, these buttons could be found on the right-hand side. I took it from the Apple macOS guidelines, since a button that triggers action is supposed to be on the very right. I could also observe that subconsciously one orientates oneself first on the right side and we are already cognitively equipped to look for main actions on the right side.

On the page where you can top up your credits by using facial images, I worked out a concept to show the user graphically instead of textually the successful upload and detection of the faces. Therefore, it allows you to see directly the detected faces, which is ready to be uploaded into the database.

When winning, I decided to emphasize this by inverting the colours and additional flashing. I divided it into two areas: standard area and decision area. The idea with the inverting was taken from Prototype V1 to visually distinguish between the two sections. The dark side with the black background should emphasize the critical decision that the user can make.

TECHNOLOGIES USED

To realize the web application, I had to plan and research everything in detail in advance to work efficiently thereafter. For the front-end, I used a client-side JavaScript web framework called Vue.js, which can be used to create single-page web applications or multipage web pages for individual sections. This progressive JavaScript framework offered me many advantages. It is quite beginner-friendly and, therefore, quick and easy to understand. I also found many tutorials that provided substantial help.

For recording states, I used a state management pattern and library for Vue.js applications called Vuex. This helped me to define application states like credits or the reward of faces among other things. Additionally, I added the vue-router package, an official router for vue.js, which is used to create routes for single-page applications. A router is needed when you need to synchronize a URL with the view of an app.

For the back-end, I used Laravel. A powerful and free PHP web framework. To handle requests from the front-end I created routes, controllers, and models. All server-side tasks are done by Laravel. I chose Laravel because it helps to create solid and maintainable web applications and drastically reduces the development effort. Especially the number of lines of code is reduced, due to ready-made standard functionalities and libraries. What was also important for me was the security aspect of the web application. Especially on the web, SQL injections, brute force attacks, and similar happenings are commonplace. Laravel has the necessary ready-made features available, which protect against the common attack points in the network. To make cheating more difficult, not all routes are directly accessible. Therefore, the user has to win to get into the actual decision area. In addition, the credits by simply changing them with the page inspector were considered. Unfortunately, you lose all credits if you update the browser manually. My next step would be to integrate a login system, which would solve this problem automatically, but unfortunately, I did not have enough time. For an easier and stable database administration, I used the MySQL server, because it is a free open source database and known for its reliability.

To make face recognition work in the browser, I used face-api.js, a JavaScript API. Face-api.js uses different types of models. For face recognition in this project, an SSD (Single Shot Multibox Detector) based on MobileNetV1 is implemented. The neural network calculates the positions of each face in an image and provides the bounding boxes together with the probability for each face. This face detector aims to achieve high accuracy in the detection of bounding box-

es for faces instead of requiring a low inference time. It was also exciting to know that the face recognition model was trained on the WIDER FACE data set. For facial recognition I used a model that is not limited to the face set used for training, i.e. it can be used for face recognition of any person.

DECISIONS

Instead of a shared web hosting solution, I decided to use a Virtual Private Server (VPS) running on a Solid State Drive (SSD). This allows for even faster performance and thus minimizes loading times for the visitor. VPS offers significant advantages over other hosting solutions, which should be utilized. All virtual servers are encapsulated, i.e. they act separately from each other, thus increasing security enormously. Since the web application is surrounded by countless sensitive facial data, it was an important decision.

During the process, the project title has changed several times. The word face, however, was always present. As a result, the name FACEPOT was created, which is derived from Jackpot. A link to Facebook can also be made since the most popular social network also deals with facial images. I saved the domain name on Namecheap and found out that facepot.com was already taken. Three top-level domains (TLD) were shortlisted: .casino, .app and .win. After a short survey, I decided to choose the TLD .win, because we all want to win. Playing a game and winning is one of life's simple pleasures. It arouses passions and can bring people together in the best way. It is also assumed that you can win something with the web application. According to GoDaddy, "Pot" is a buzzword of high value, which achieves an average sales price of CHF 2'159.00. Furthermore, "Face" is a frequently used keyword and "Facepot" is memorable.

I carefully considered whether the visitors will obtain raw aligned and cut facial images or rather faceprints consisting only of numerical numbers. I decided on the first one because, thanks to the conversations and research on the internet, I found out that the faceprints could vary between the individual companies, for example, and thus make the exchange more difficult. Therefore, I was looking for a compromise in which everyone could use the data. With the help of UTKFace dataset, I tested the reactions. The endless list of numbers did not yield the same effectiveness as a large number of facial images. Besides, the raw data face images contain the original data of the shot, which at the same time are already prepared for benchmarking an algorithm when uploading and downloading on FACEPOT.

I wanted to keep the game very simple without distracting the visitors too much from the topic. I decided on a three-reel slot machine with a very simple payout table. As soon as the fictitious face symbol stops, you get a payout in the form of raw face images. This payout increases the more of these symbols stop. In the implementation, the winning logic played a crucial role. To keep the motivation up, I tried to keep the visitors on their toes with small winnings, so that they don't give up quickly and instead kept playing. The chance of winning had to be adjusted continuously and I decided furthermore not to win a fixed number of facial images from the face pot but in percentage so that the face pot never gets empty. The corresponding facial images that were won are automatically deleted from the database of the web application to ensure their uniqueness.

To set the reels with the symbols in motion, the "Spin button" must be clicked. You need credits for this. The credits can be topped up using the "Insert Face/s button". For each face that is uploaded and accepted, you will receive one credit. It is also possible to upload single photos with multiple faces, which will automatically count the faces and crop and align them accordingly. I played a scenario, which pictures the visitors would upload. Some of them tried to upload the same face photo or a photo that didn't contain a face. This observation helped me to optimize it. Therefore, I can ensure a clean, unique face data set, which preserves the value.

FINAL FEEDBACKS

In general, the feedback was mostly positive, but there were also some points of criticism. Many of the respondents felt that the result was an unconventional way of communicating this critical topic to a wider audience. Fortunately, in their opinion, it makes one think about how we deal with photos arbitrarily, often ending up on the internet without their knowledge or consent. This was my main goal to achieve that, to increase their existing awareness and encourage them to question the development and influence in the near future.

Some of them did not even dare to upload photos of themselves, let alone put others at risk. They had to think several times whether they would do it or not. In their opinion a paradoxical consideration, although they never do exactly that in their daily lives. Many revealed that they are not aware that photos are no longer just photos, but data that could be interesting for certain applications.

In the subreddit r/critical design I also received the feedback that the result was solid but the execution could have been more informative. It also comes across as too sterile. This was clear to me from the beginning that this could be a disadvantage or a problem if I endeavour with all means to make this topic as neutral as possible so that the users can form their judgements. Perhaps it would have made more sense to influence them a bit more to make the required decisions after the win.

FACEPOT.WIN

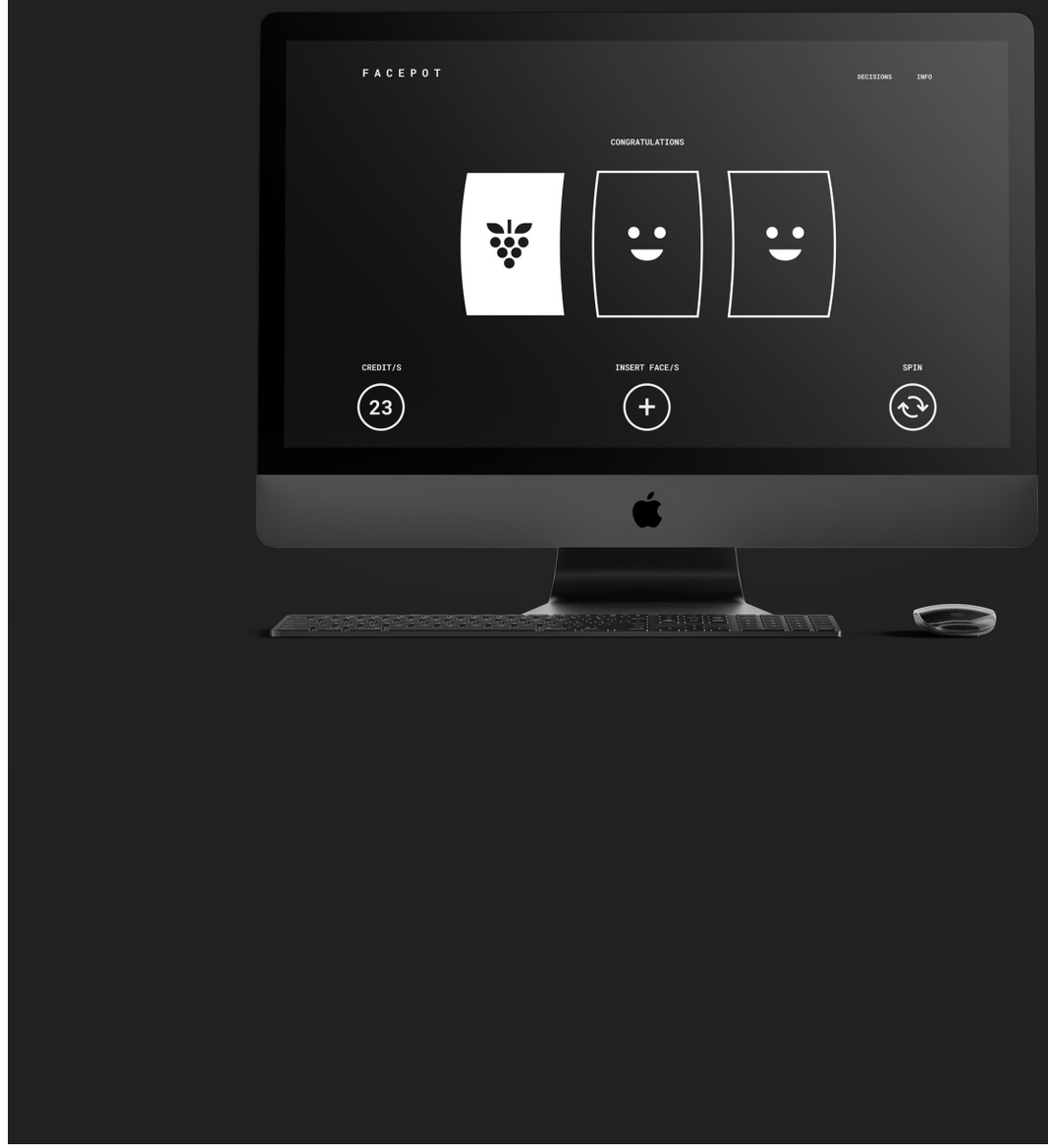

Figure 16. FACEPOT Win (Source: Own representation)

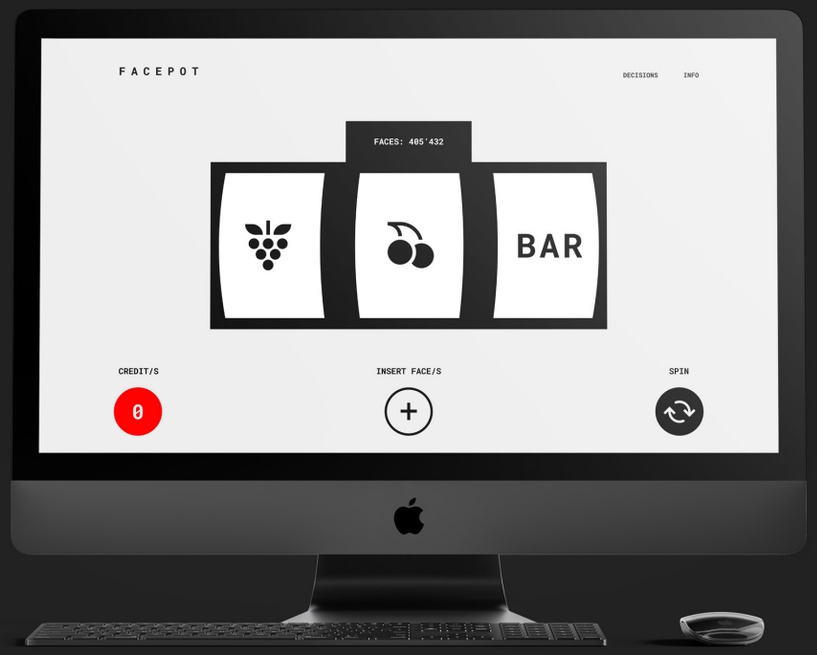

Figure 17. FACEPOT Slot Machine (Source: Own representation)

Figure 18. FACEPOT Insert Face/s (Source: Own representation)

Figure 19. FACEPOT Decision (Source: Own representation)

Figure 20. FACEPOT Decision 2 (Source: Own representation)

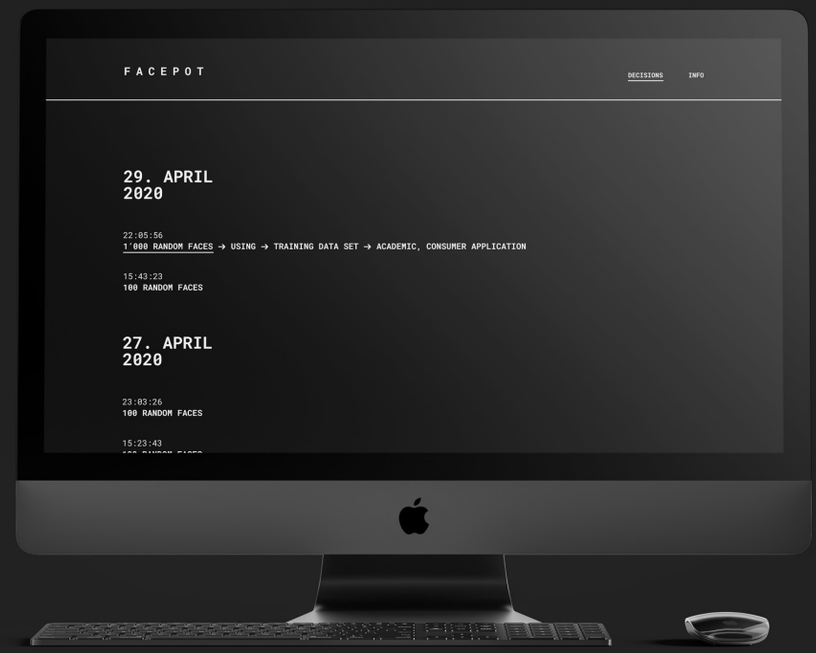

Figure 21. FACEPOT Decisions (Source: Own representation)

IV

CONCLUSION AND REFLECTION

LEARNINGS

The last few months have been very intense and have been difficult and instructive at the same time.

I did not shy away from learning something completely new for the theoretical part, from making more effort with the attitude than I would have chosen a subject area where knowledge already exists. In the initial phase, I explored various subject areas that had a particularly strong correlation between man and machines.

Therefore, at the beginning, I pursued an overly speculative direction, exploring the interaction between a computer with a mind and its operator. However, based on feedback and conversations, I realized that a very speculative topic is very difficult for outsiders to understand. As a result, I lacked facts on which to base my findings and I interpreted far too much into it on my own. Therefore, my ideas and plans were often not understood.

I will keep this insight in mind for future projects, while integrating people in the process continuously, and gathering their input instead of just relying on my thoughts and ideas. I started to use this approach in the prototypes of this bachelor thesis, and even then, I noticed that relatively few people were still involved in the development of the first two prototypes. I changed this in the second and third prototypes, evaluated the opinions, and tried to understand their perspective to build on it and optimize the prototypes accordingly.

I also noticed how difficult it was for me not to work in a team where people can support and motivate each other. Especially in the current challenging times, in new normality due to the COVID-19 pandemic, this made it even more difficult. I completely missed the direct exchange and it taught me to appreciate this even more. During the final implementation phase with the tight period, I noticed intensively that despite mature planning and commitment, this could not be compensated for. Therefore, I would have liked to work further on some areas (see Future Steps on page 84).

Surprisingly, I also encountered something exciting. I never noticed it throughout my studies. For example, when I wanted to convey an idea using visual aids, such as a sophisticated and highly polished mockup, the respondents often generated unspecific questions and answers about the aesthetics instead of the core idea. Unfortunately, I discovered this too late, but better than never. Therefore, I will sketch more in the future and use this as a quick explanatory aid, which will allow the respondents to concentrate on the essential aspects instead of distracting and overburdening them with the visuals. The right time should also be considered the current stage of the project must be indicated to prevent misconceptions.

During my studies, I was able to gain some experience in front-end web development. To make an application work, it is necessary to have the back-end, which takes care of the implementation of the functions. For my bachelor thesis, I had to view many tutorials, trying things out, and receiving support from open communities on the internet. This led me to learn much in the back-end area. This was the greatest challenge of my work, which required a significant time and effort, although it paid off in the end. It was important to me that at least the main function of the web application was functioning so that the audience could interact with it.

CONTRIBUTION

As a prospective interaction designer, dealing with this topic was both fascinating and, at the same time, worrying. The topic will particularly affect interaction designers in the area of user experience, and they will need to keep an eye on the responsibility and consequences and think in all categories. Biometric technologies, such as face recognition, increasingly influence daily habits and consumption in a tailor-made way. Moreover, it can be used in unimaginable and not yet existing areas of application. The field is, therefore, still very wide open. Already today we are getting used to applications in which it is already implemented and practically don't notice it anymore. FaceID developed by Apple showed the masses in 2017 that face recognition technology exists and works.

Currently, we are in a situation where it is crucial to act early to contain potential risks while respecting personal rights and privacy. This should involve all parties, whether it is developers, researchers, users, or the government.

I followed a critical theory-based design approach to challenge the assumptions and ideas about the role of biometric facial data in everyday life. It was a challenge to make the abstract intangible topic tangible for a broad audience. Therefore, I tried to give an impulse with my work that should raise awareness and make people think about it. My work offers the chance to gain the collected facial data as well as the power over them to question the real value of this data. To entice users to question their use of personal photos of faces, which is put at risk every day in the world. A face contains extensive information that is so unique to a person that the use of face recognition technology is perceived as very personal. Every time a face appears on the internet, it may become part of a facial recognition database. This collective mania is changing the meaning of the human face dramatically. It can be seen as a new kind of currency.

Despite the complexity of the topic, I tried to get a more detailed overview and mostly questioned the development and distribution of these systems as well as people's awareness of how to handle their facial data. I concluded that the face is a valuable and sensitive source of data in this fast and strongly developing time in the field of computing power and artificial intelligence.

Facial data can tell a simple app developer more than the human eye can see with the help of facial recognition technology. Forrester's Khatibloo, for example, notes that researchers have used facial recognition technology to determine the sexual orientation of people based solely on normal photos with a very high success rate. He explained, however, that while this study has its limitations, the technology will leapfrog much faster than consumers and regulators will realize. When I think about it, the potential for misuse is limitless. That is why it justifies obtaining a special permit, which should be critically evaluated by the data protection commissioners to contain the potential for malpractice.

"Fate is written in the face" (Fellini, n.d.).

This normality can build a future in which we become powerless over a form of surveillance that goes far beyond anything we have known up to now. As we know, we have only one face, and it is not something that can be easily changed.

Before my studies, I saw every new technology as useful and as progress for mankind, where the advantages outweigh the disadvantages. During my studies and especially while working on this topic I concluded that new technologies with its design decisions only reveal their real impact on society over time and after some clarification. This has opened my eyes, which will accompany me for the rest of my life.

FUTURE STEPS

Based on a priority list, I worked through the most important functions. Although I finished my bachelor project, I would like to mention that there are still some points that I would like to improve and add.

I would have liked the landing page, or rather the first page for new visitors, to have worked out further. Since it was a very tight period to develop a web application with limited experience, I reduced this start page to the minimum, so that the visitors still understand briefly and concisely what the website is all about. My first next step would be to make the start page more inviting and exciting so that the visitor becomes familiar with the site despite the critical topic. It is, therefore, conceivable to equip this site with scrolling events including animations or illustrations, which take up the topic even further. The first impression is especially important.

Also when uploading the pictures, my future step would have been to show the user several hints visually, for example, if the face is already in the database, the file is too large, unknown or wrong file type is selected, more than 120 pictures are uploaded at once or the face is not recognized. I implemented this at the beginning and took it out again according to the user feedback because too many hints appeared at once and disturbed the interactive elements visually. Here I would have liked to work out a concept that is aesthetically simple and easy to understand.

Finally yet importantly, it would have been interesting to work out something additional after the decision and after downloading., for example, a platform where users can exchange or sell the facial images they have won to make it even more informative.

V BIBLIOGRAPHY

REFERENCES

BOOKS

Bridle, J. (2018). New Dark Age. London, UK: Verso.

Chollet, F. (2017). Deep Learning with Python (1st ed.). Shelter Island, New York: Manning Publications.

Cipolla, R., & Pentland, A. (1998). Computer Vision for Human-Machine Interaction (1st ed.). Cambridge, United Kingdom: Cambridge University Press.

Davies, E. R. (2017). Computer Vision: Principles, Algorithms, Applications, Learning (5th ed.). Amsterdam, Netherlands: Amsterdam University Press.

Dawson-Howe, K. (2014). A Practical Introduction to Computer Vision with OpenCV (Wiley-IS&T Series in Imaging Science and Technology) (1st ed.). Hoboken, NJ, United States: Wiley.

Jacobsen, K. L. (2015). Humanitarian biometrics. In The Politics of Humanitarian Technology (pp. 57–86). Abingdon, UK: Routledge.

Maeda, J. (2019). How to Speak Machine: Computational Thinking for the Rest of Us (2nd ed.). Unknown, Unknown: Portfolio/Penguin.

Mueller, J. P., & Massaron, L. (2019). Deep Learning For Dummies (For Dummies (Computer/Tech)) (1st ed.). Hoboken, New Jersey: For Dummies.

Rosebrock, A. (2017). Deep Learning for Computer Vision with Python. Unknown, Unknown: PyImageSearch.

Rouhiainen, L. (2018). Artificial Intelligence. Zaltbommel, Netherlands: Van Haren Publishing.

PAPERS

Federal Trade Commission. (2012). Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies. Retrieved from http://www.ftc.gov/os/2012/10/121022facialtechrpt.pdf

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444. https://doi.org/10.1038/nature14539

Pereira, G., & Moreschi, B. (2019). Ways of Seeing with Computer Vision: Artificial Intelligence and Institutional Critique. Ways of Seeing with Computer Vision: Artificial Intelligence and Institutional Critique, 28–33. https://doi.org/10.33767/osf.io/nv9z2

Stiftung für Effektiven Altruismus. (2015, December 12). Künstliche Intelligenz: Chancen und Risiken. Retrieved 2 March 2020, from https://ea-stiftung.org/s/Kunstliche-Intelligenz-Chancen-und-Risiken.pdf

United States Government Accountability Office. (2015). FACIAL RECOGNITION TECHNOLOGY: Commercial Uses, Privacy Issues, and Applicable Federal Law (GAO-15-621). Retrieved from https://www.gao.gov/assets/680/671764.pdf

Das, A., Degeling, M., Wang, X., Wang, J., Sadeh, N., & Satyanarayanan, M. (2017). Assisting Users in a World Full of Cameras: A Privacy-Aware Infrastructure for Computer Vision Applications. 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 1–10. https://doi.org/10.1109/cvprw.2017.181

ARTICLES

Cino, J. G. (2017, April 5). Facial recognition is increasingly common, but how does it work? Retrieved 10 April 2020, from https://theconversation.com/facial-recognition-is-increasingly-common-but-how-does-it-work-61354

Collie, M. (2019, July 19). Just walk away from it: The scary things companies like FaceApp can do with your data. Global News. Retrieved from https://globalnews.ca

Davis, W. (2020, February 26). Digital News Daily: Clearview Data Breach Prompts Renewed Calls To Curb Facial Recognition. Retrieved 10 April 2020, from https://www.mediapost.com/publications/article/347682/clearview-data-breach-prompts-renewed-calls-to-cur.html

Dickson, B. (2020, February 27). Deep learning advances are boosting computer vision — but there's still clear limits. Retrieved 2 March 2020, from https://thenextweb.com/neural/2020/02/26/computer-vision-applications-the-power-and-limits-of-deep-learning-syndication/

Dieffenbacher, C. (2019, May 13). Wie uns Maschinen sehen. Retrieved 2 March 2020, from https://www.aargauerzeitung.ch/kultur/buch-buehne-kunst/wie-uns-maschinen-sehen-134470802

Fowler, G. A. (2019, May 23). Analysis: Apple is sharing your face with apps. That's a new privacy worry. Retrieved 27 May 2020, from https://www.chicagotribune.com/business/blue-sky/ct-apple-facial-recognition-privacy-20171202-story.html

Harding, D. (2019, July 22). Facial Recognition: When Convenience and Privacy Collide. Retrieved 10 April 2020, from https://www.securitymagazine.com/articles/90533-facial-recognition-when-convenience-and-privacy-collide

Kofman, A. (2016, October 13). LOSING FACE: How a Facial Recognition Mismatch Can Ruin Your Life. Retrieved 10 April 2020, from https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/

LaFrance, A. (2017, March 27). Who Owns Your Face? Retrieved 10 April 2020, from https://www.theatlantic.com/technology/archive/2017/03/who-owns-your-face/520731/

Lange, C. (2018, June 4). Surveillance, Bias and Control in the Age of Facial Recognition. Retrieved 10 April 2020, from https://frieze.com/article/surveillance-bias-and-control-age-facial-recognition-software?language=de

Mettler, S. H. J. (2020, January 22). Gesichtserkennung Clearview: Der Albtraum für die Privatsphäre. Retrieved 4 May 2020, from https://www.tagesanzeiger.ch/digital/internet/gesichtserkennung-clearview-der-albtraum-fuer-die-privatsphaere/story/31072705

Metz, C. (2019, July 13). Facial Recognition Tech Is Growing Stronger, Thanks to Your Face. Https://Www.Nytimes.Com/#publisher. Retrieved from https://www.nytimes.com

Murgia, M. (2019, September 18). Who's using your face? The ugly truth about facial recognition. Retrieved 4 May 2020, from https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e

Nilsson, P. (2019, October 30). Face off: the perils of sharing your biometric data. Financial Times. Retrieved from https://www.ft.com

Rachel Metz, CNN Business. (2019, April 19). If your image is online, it might be training facial-recognition AI. Retrieved 4 May 2020, from https://edition.cnn.com/2019/04/19/tech/ai-facial-recognition/index.html

Schurter, D. (2019, July 26). FaceApp: iPhone- und Android-App aus Russland wirft Fragen auf. Retrieved 10 April 2020, from https://www.watson.ch/digital/apps/437721592-faceapp-iphone-und-android-app-aus-russland-wirft-fragen-auf#h4_7

Selinger, E., & Hartzog, W. (2016, May 7). Wenn Selfies zu Überwachungsmerkmalen werden. Retrieved 10 April 2020, from https://www.schirn.de/magazin/kontext/hartzog_selinger_surveillance_faceprint/

Solon, O., & Murphy, J. (2019, March 17). Facial recognition's 'dirty little secret': Social media photos used without consent. Retrieved 10 April 2020, from https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921

The Guardian. (2019, September 2). Chinese deepfake app Zao sparks privacy row after going viral. Retrieved 4 May 2020, from https://www.theguardian.com/technology/2019/sep/02/chinese-face-swap-app-zao-triggers-privacy-fears-viral

Vincent, J. (2019, May 10). A photo storage app used customers' private snaps to train facial recognition AI. Retrieved 10 April 2020, from https://www.theverge.com/2019/5/10/18564043/photo-storage-app-ever-facial-recognition-secretly-trained-ai

Webb, K. (2019, July 18). Viral app that makes you look old with shocking precision may be quietly keeping all your data. Retrieved 10 April 2020, from https://www.businessinsider.com/faceapp-privacy-data-terms-service-russia-2019-7?r=US&IR=T

ACADEMIC THESIS

Lawrence, R. G. (1980). Machine Perception of Three-Dimensional Solids (Master's thesis, Massachusetts Institute of Technology, 1963) (pp. 8-24). New York: Garland Publishing.

WEBSITES

Brownlee, J. (2019, July 5). A Gentle Introduction to Computer Vision. Retrieved 2 March 2020, from https://machinelearningmastery.com/what-is-computer-vision/

Bube, L. (2019, March 29). Künstliche Intelligenz im Wandel der Zeit: »Eine kurze Geschichte der KI«. Retrieved 2 March 2020, from https://www.crn.de/software-services/eine-kurze-geschichte-der-ki.119602.2.html

C. (2020, April 21). This Person Does Not Exist - how does it work? – Retrieved 4 May 2020, from https://www.machinecurve.com/index.

php/2019/07/17/this-person-does-not-exist-how-does-it-work/

Computer Vision. (n.d.). Retrieved 2 March 2020, from https://www.ibm.com/topics/computer-vision

Computer Vision: Was es ist und was man darüber wissen sollte. (n.d.). Retrieved 2 March 2020, from https://www.sas.com/de_ch/insights/analytics/computer-vision.html#industries

COMPUTER-VISION. (2020, February 26). Retrieved 2 March 2020, from https://www.lexoro.ai/kompetenzfelder/computer-vision/

Cubera Solutions AG. (2018, April 5). Gesichtserkennung im Dienstleistungssektor. Retrieved 19 April 2020, from https://www.cubera.ch/referenzen/projekte/gesichtserkennung-im-dienstleistungssektor/

Cubera Solutions AG. (2019, December 11). Who is it? Gesichtserkennung - Projekte Showcase. Retrieved 19 April 2020, from https://www.cubera.ch/referenzen/projekte/who-is-it/

Entropic. (2019, January 9). The Food of Facial Recognition: Your Regularly Updated Photos & Videos. Retrieved 10 April 2020, from https://www.scentropic.com/blog/2019/jan/facial-recognition-sources/facial-recognition-sources.shtml

Essbaumer, A. (2018, March 22). Computer Vision mit Deep Learning: Die visuelle Wahrnehmung der künstlichen Intelligenz. Retrieved 2 March 2020, from https://www.capgemini.com/de-de/2018/03/computer-vision-deep-learning-auge-der-kuenstlichen-intelligenz/

Facial Recognition Market Size | Industry Report, 2020-2027. (n.d.). Retrieved 4 May 2020, from https://www.grandviewresearch.com/industry-analysis/facial-recognition-market

Global, B. (2020, March 2). Fahrerassistenzsysteme unterstützt durch künstliche Intelligenz: der nächste Schritt in Richtung automatisiertes Fahren. Retrieved 2 March 2020, from https://www.bosch.com/de/stories/computer-vision/

Kapoor, A. (2019, February 25). Deep Learning vs. Machine Learning: A Simple Explanation. Retrieved 2 March 2020, from https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08

Luber, S, & Litzel, N. (2017, April 26). Was ist Deep Learning? Retrieved 2 March 2020, from https://www.bigdata-insider.de/was-ist-deep-learning-a-603129/

Maschinelles Sehen Definition & Erklärung | Informatik Lexikon. (2019, December 23). Retrieved 2 March 2020, from https://www.informatik-verstehen.de/lexikon/maschinelles-sehen/

Nicolls, D. (2019, November 21). What is Biometric Authentication? Retrieved 10 April 2020, from https://www.jumio.com/what-is-biometric-authentication/

PYMNTS. (2019, May 9). Storage App Used Photos To Train Facial Recognition Software. Retrieved 10 April 2020, from https://www.pymnts.com/news/security-and-risk/2019/ever-photo-app-facial-recognition-ai/

Rodriguez, R. (2020, March 11). 6 Disadvantages of Facial Recognition You Need to Be Aware of. Retrieved 10 April 2020, from https://techbusinessguide.com/disadvantages-facial-recognition/

Symanovich, S. (n.d.). How does facial recognition work? Retrieved 10 April 2020, from https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

Szczys, M. (2019, August 25). The Tens Of Millions Of Faces Training Facial Recognition; You'll Soon Be Able To Search For Yourself. Retrieved 4 May 2020, from https://hackaday.com/2019/08/25/the-tens-of-millions-of-faces-training-facial-recognition-youll-soon-be-able-to-search-for-yourself/

The Complete Guide to Facial Recognition Technology - Panda Security. (2019, October 15). Retrieved 10 April 2020, from https://www.pandasecurity.com/mediacenter/panda-security/facial-recognition-technology/

Thilakarathne, H. (2018, August 12). Deep Learning Vs. Traditional Computer Vision. Retrieved 2 March 2020, from https://naadispeaks.wordpress.com/2018/08/12/deep-learning-vs-traditional-computer-vision/

«Unser Ziel ist es, sichere autonome Autos zu entwickeln». (2020, January 7). Retrieved 2 March 2020, from https://ee.ethz.ch/de/news-und-veranstaltungen/d-itet-news-channel/2020/01/our-goal-is-to-develop-safe-autonomous-cars.html

BLOGS

A. (2018a, April 2). Introduction to computer vision: what it is and how it works. Retrieved 2 March 2020, from https://algorithmia.com/blog/introduction-to-computer-vision

C. (2018b, June 18). Beginner's Guide to Computer Vision. Retrieved 2 March 2020, from https://medium.com/readers-writers-digest/beginners-guide-to-computer-vision-23606224b720

Calomme, V. (2019, February 7). Die Geschichte der Künstlichen Intelligenz - welove.ai. Retrieved 2 March 2020, from https://www.welove.ai/de/blog/post/geschichte-kuenstlicher-intelligenz.html

Dickson, B. (2018, March 16). The security and privacy risks of face recognition authentication. Retrieved 10 April 2020, from https://bdtechtalks.com/2017/10/21/face-recognition-faceid-security-privacy-concerns/

Dwyer, B. (2019, May 3). Face-controlled apps are here — and they are about to transform how we interact with our devices. Retrieved 10 April 2020, from https://medium.com/@braddwyer/face-controlled-apps-are-here-b1c6eb4a3e27

Grossfeld, B. (2020, February 19). Deep learning vs machine learning: a simple way to understand the difference. Retrieved 2 March 2020, from https://www.zendesk.com/blog/machine-learning-and-deep-learning/

I. (2018c, April 17). Biometric Recognition: definition, challenge and opportunities of biometric recognition systems. Retrieved 10 April 2020, from https://medium.com/iquii/biometric-recognition-definition-challenge-and-opportunities-of-biometric-recognition-systems-d063c7b58209

Padhan, A. (2020, January 7). What is computer vision? What are its applications? Retrieved 2 March 2020, from https://www.skyfilabs.com/blog/what-is-computer-vision

Singh, R. (2019a, June 8). Computer Vision — An Introduction. Retrieved 2 March 2020, from https://towardsdatascience.com/computer-vision-an-introduction-bbc81743a2f7

Singh, R. (2019b, November 16). Visual Perception-From Human Vision to Computer Vision. Retrieved 2 March 2020, from https://medium.com/towards-artificial-intelligence/visual-perception-from-human-vision-to-computer-vision-3152134292

PRESENTATIONS

Blattner, M. (2020). Neuronale Netze und das Black Box Problem. Presentation, Online.

Yogeshwar, R. (2020). Künstliche Intelligenz: Perspektiven und Visionen. Lecture, Zurich University of the Arts.

VIDEOS

CrashCourse. (2017, November 15). Computer Vision: Crash Course Computer Science #35 [Video file]. Retrieved from https://www.youtube.com/watch?v=-4E2-0sxVUM

Function. (2019, February 21). How Facial Recognition Works - 'Where's Waldo' (Humans vs. Laptop) [Video file]. Retrieved from https://www.youtube.com/watch?v=kbniJ0WWAdM&feature=youtu.be

Li, F. (2015, March 1). How we're teaching computers to understand pictures [Video file]. Retrieved from https://www.ted.com/talks/fei_fei_li_how_we_re_teaching_computers_to_understand_pictures#t-1026768

Quarks (Producer), Wolff, T. (Director) & Yogeshwar, R. (Director). (2019). Der grosse Umbruch - Wie Künstliche Intelligenz unser Leben verändert [Motion Picture]. WDR Fernsehen https://www1.wdr.de/mediathek/video/sendungen/video-der-grosse-umbruch--wie-kuenstliche-intelligenz-unser-leben-veraendert-100.html

Surbeck, W. F. I. (2018, February 21). Biometrische Daten - Digitale Gesichtserkennung zunehmend auch in der Schweiz [Video file]. Retrieved from https://www.srf.ch/news/schweiz/biometrische-daten-digitale-gesichtserkennung-zunehmend-auch-in-der-schweiz

The Economist. (2017, November 1). Facial recognition technology will change the way we live | The Economist [Video file]. Retrieved from https://www.youtube.com/watch?v=nT_PXjLol_8

The Hated One. (2020, February 19). Why biometric security fails at being secure [Video file]. Retrieved from https://www.youtube.com/watch?v=tJw2Kf1khIA

Vox. (2019, December 10). What facial recognition steals from us [Video file]. Retrieved from https://www.youtube.com/watch?v=cc0d-qW2HCRc&t=241s