Universiteit Leiden
The Netherlands

Opleiding Informatica

Minority Report at the border:

An ethical analysis of the iBorderCtrl-project

Rutger Doting

Supervisors:
Prof. dr. M.E.H. van Reisen
Dr. L.E.M. Taylor

BACHELOR THESIS

Leiden Institute of Advanced Computer Science (LIACS)
www.liacs.leidenuniv.nl

21/07/2021

Abstract

The iBorderCtrl-project was an EU-funded project that ran from 1 September 2016 until 31 August 2019, and aimed to improve the efficiency of border crossings by a variety of technological solutions. Two of these technologies, facial recognition and AI lie detection, raise immediate ethical questions. This thesis aims to discuss these ethical questions by conducting an ethical analysis. In our analysis, we use the three main ethical theories, consequentialism, deontology and virtue ethics, to provide a theoretical framework. We found that all of the ethical theories think that the application of the technologies used in the iBorderCtrl-project is unethical, be it in different degrees and for different reasons. Therefore, we conclude that the application of these technologies is unethical.

Contents

1 Introduction

In recent years the discussion of "ethical AI" has gained the attention of the general public, technologists and policy makers. However, it is not entirely clear which ethical considerations will be seen as relevant, and, to quote Dr. Petra Molnar from section 7, "Who's ethics are we even talking about?". This thesis is an attempt to provide the beginning of an ethical process that can hopefully be used to determine whether the application of a certain technology is ethical or not. This will be achieved by means of a comparative analysis of the iBorderCtrl-project, in which we use the three main ethical theories to determine whether this project will be seen as ethical.
The iBorderCtrl-project was a project by the iBorderCtrl consortium, coordinated by a company called European Dynamics, that aimed to make crossing EU borders more efficient [iBo21] [Eur18]. For this, the consortium received 4.5 million euros from the EU Horizon 2020 program. The project was tested at the Greek, Hungarian and Latvian borders [iBo21], in coordination with police forces and border guards of those countries. While the project itself was supported and even promoted by the European Commission (see [Eur18]), the legality of the technologies remains vague. This is even acknowledged by the project itself, since they say on their website:

"It should be also noted that some technologies are not covered by the existing legal framework, meaning that they could not be implemented without a democratic political decision establishing a legal basis." [iBo21, Frequently Asked Questions]

Therefore, the legal basis of the iBorderCtrl-project is uncertain. However, borders are a relatively opaque place with regards to legal rights, as Dr. Petra Molnar explains: "[the border space is] a space of discretionary decision making where states in particular are able to move away from certain rights because they are able to say: "Oh well, it's at the border, it's national security"" Therefore, even though the legality of some of the technologies of the iBorderCtrl-project is disputed, the European Commission still argued that the project as a whole is legal. In this thesis, we will focus on the ethics of the project, instead of discussing the legality of the project. It should be noted that this analysis will be relatively high-level, due to the constraints on the length of the thesis set by the Leiden Institute of Advanced Computer Science, which allows the thesis to be roughly 25 pages. This is sufficient for the description of a scientific experiment and the corresponding data, but not for an in-depth philosophical analysis. However, we hope that our high-level analysis will be an interesting starting-point for further discussion.

1.1 Thesis overview

This section contains the introduction; Section 2 discusses related work; Section 3 outlines our methodology; Section 4 describes the theoretical framework we have used; Section 5 describes the technologies of the iBorderCtrl-project that we have analysed; Section 6 describes the applications of these technologies; Section 7 describes the perception of resource persons of the iBorderCtrl-project; Section 8 contains our ethical analysis; Section 9 concludes our thesis. For the reader's convenience, we have included a table – table 1 – with the encountered abbreviations and their meaning.
This bachelor thesis was written as part of the bachelor degree at the Leiden Institute of Advanced Computer Science (LIACS), and was supervised by prof. dr. M.E.H. van Reisen and dr. L.E.M Taylor.

Abbreviation	Meaning	Explanation of term
GDPR	General Data Protection Regulation	Privacy and data protection law of the European Union
FNIR	False Negative Identification Rate	Type II error rate. A Type II error is made when the null hypothesis is not rejected when it should be rejected
NFP	Fixed Number of False Positives	Fixed number of false positives
NIST	National Institute of Standards and Technology	Science laboratory in the United States

Table 1: Meaning of abbreviations

2 Related work

The field of the ethics of technology is relatively young, since it is naturally connected with the technologies that it is studying. This means that until recently, there was less research into this topic than into other topics of philosophy. However, as it has become clear that the impact of technology on society is rapidly growing, the research into the ethics of technology has greatly increased. In this section, we will discuss the relevant literature that is in some way connected with the iBorderCtrl-project. We have divided the literature into three relevant subsections, to have a clear separation of the various topics in the literature that are relevant to our discussion. These three topics are: the ethics of algorithms, the ethics of artificial intelligence, and the application of virtue ethics to technology. We will start with a discussion of the ethics of algorithms, before moving on to the strongly connected ethics of artificial intelligence. We will conclude with a discussion of the application of virtue ethics to technology.

2.1 Ethics of algorithms

Algorithms play an increasingly important role in our daily lives, as can be seen in the very enlightening book *Weapons of Math Destruction*, by Cathy O'Neill [O'N16]. Therefore, it is important to understand any ethical decisions these algorithms might be implicitly making, since these decisions will have significant consequences. In [KvP11], the authors argue that some algorithms are value-laden, which means that these algorithms have certain values built into them by design. They use medical algorithms as an example, where a decision to mark a human cell as diseased or not is based on the programmer's wish to avoid either false positives or false negatives. The authors argue that this decision depends on value-judgements. This is an example in which implicit value-judgements alter the result of the algorithm, which can have significant consequences – in this case, whether a disease is detected in time. Thus, value-laden algorithms make decisions that have ethical consequences, so there is an ethics of algorithms.
To help us understand the ethical concerns raised by these algorithms, we follow [MAT+16], where an overview is given of the ethical debate about algorithms and algorithmic decisions. The paper outlines six types of ethical concerns raised by algorithms, which are very useful to our discussion. These concerns are: (1) Inconclusive evidence, (2) Inscrutable evidence, (3) Misguided evidence, (4) Unfair outcomes, (5) Transformative effects and (6) Traceablity.

2.2 Ethics of artificial intelligent systems

Closely connected with the ethics of algorithms, is the ethics of artificial intelligent systems, which likewise are gaining in prominence. [Spa07] discusses the ethics of artificial intelligence systems by examining who would be responsible for the actions of these systems. Sparrow uses the example of a war crime committed by an autonomous artificial intelligence system as a starting point for his search for responsibility. According to Sparrow, none of the actors, which include programmers, commanding officers and the system itself, can be seen as ultimately responsible. Since responsibility for crimes is a necessary condition of a just war, Sparrow concludes that it is unethical to use autonomous artificial intelligence systems in war. Without pre-empting the discussion of this thesis, it might be possible to widen the scope of this conclusion, and say that responsibly for decisions if a necessary condition of a just society, and therefore that it it unethical to use autonomous artificial intelligence systems in society.

Especially relevant to our discussion is [SHLH21], where the authors examine the potential societal harm that could be caused by AI lie detection. They do this by conducting a survey of 129 individuals, and asking them about their perspective on AI lie detection. They found that consent and accuracy are the major factors of concern for the individuals surveyed. In regards to societal harm, they found that accurate thought exposing, which they define as "using a device to predict an individuals inner thoughts" [SHLH21, p. 2], is mostly unregulated. To safeguard the individual, they propose a ban on "mental trespassing", or "non-consensual use of thought exposing technology" [SHLH21, p. 2].

2.3 Technology and virtue ethics

The application of virtue ethics to technology can be seen as a novel approach, even in such a young field as the ethics of technology. However, this does not mean that there are not yet interesting ethical approaches. The most relevant to our discussion is [Val16]. In this book, Vallor is searching for an ethical framework to deal with the challenge of what she calls "acute sociotechnical opacity" [Val16, p. 6] in the 21st century, which means that "the practical circumstances of our everyday lives are changing so rapidly due to technological innovations that we cannot reasonably anticipate the impact of future states of affairs on our morality" [Rei19, p. E–18]. In response to this challenge, she develops a framework that is based on the cultivation of "technomoral" virtues; twelve virtues that help humans live well with emerging technology. These virtues can be seen in table 2. We will use these virtues extensively in our virtue ethics analysis of the technologies of iBorderCtrl.

3 Methodology

The methodology of this thesis has two main parts: reviewing the literature (section 3.1), and interviewing resource persons (section 3.2). Both of these methods play an important role in the finalisation of the thesis, and I will go into depth about each method in the following subsections.

3.1 Literature review

The literature review is a continually updating process of reading and re-reading relevant literature. This is tightly connected with the interviewing of resource persons, since each interview has to be prepared beforehand by reading the relevant literature, and each interview in turn generates new interesting literature. This means that our literature reading process looks like this:

- Read relevant literature found about the interviewee's area of expertise
- Conduct interview
- Read literature recommended by interviewee

Besides these "natural" forms of literature recommendations, we also conducted our own research about this topic, beginning with recent literature on topics of interests, for example, [Val16] and using that literature as a stepping stone to other relevant research, by seeing which papers are referenced there.
For this literature review, we used a few criteria for selecting the literature. First of all, the literature should be relevant to the iBorderCtrl-project. By relevant to the project, we mean that the literature should be about one of the technologies we discuss, AI lie detection or facial recognition, or a related topic, for example artificial intelligence in general.
The second criterion, which we used for the technology-specific topics in particular, is that the literature should be relatively recent, since the capabilities of these technologies are rapidly expanding, which means that new ethical questions arise out of the new possibilities offered. Therefore, we focused on literature from after the year 2005. We have chosen 2005 as a useful cut-off point, but there is no special significance to this year, it only serves as a way to classify the literature into "relatively recent" and "too old".
The third criterion we used, it that all the literature we included should be published in a peer-reviewed journal, or at least should be peer-reviewed in some other way. This way, we can be sure that the literature complies with the latest standards in scientific publishing, and has been reviewed by experts.
Based on these three criteria, we decided to focus on literature that concerns the ethics of algorithms, the ethics of artificial intelligence, Vallor's technosocial virtues, and literature about the technical specifications of the technologies used in the iBorderCtrl-project. We did not include the literature of consent and the legal bases of the General Data Protection Regulation (GDPR), since these are legal questions that are out of our areas of expertise. Therefore, we decided to limit the scope of our literature review to only the aforementioned topic.

3.2 Interviews with resource persons

Another method we use to get a better understanding of the iBorderCtrl-project and about the theories we are researching, is conducting a series of interviews with so called "resource persons".

A resource person is an expert in a specific field, who can be called upon to provide information. In the context of the iBorderCtrl-project these include digital rights activists, academics and politicians. We use these interviews in an exploratory sense, which means that we use them to elucidate what the iBorderCtrl-project is doing specifically, and what certain ethical theories might say about this. We do not use these interviews to draw general conclusions about the opinion of the iBorderCtrl-project of the public at large, since the number of persons interviewed is too small for that kind of inference.
We selected the interviewees based on the number of times their names came up in articles about the iBorderCtrl-project. We also used the https://iborderctrl.no/act website to get a good understanding of who is concerned about the iBorderCtrl-project. Based on these two sources, we contacted a group of people who had engaged with the iBorderCtrl-project in some way. The people contacted (in chronological order) include:

- Rop Gonggrijp (Founder of the Dutch internet service provider XS4ALL, activist)
- Dr. Vera Wilde (Expert on lie detection)
- Dr. Petra Molnar (Human rights and refugee lawywer)
- Dr. Patrick Breyer (MEP for the German Pirate Party)
- Sophie in 't Veld (MEP for the Dutch D66)
- Konstantinos Kakavoulis (Staff member of Homo Digitalis, the Greek digital rights organisation)
- Dr. James O'Shea (Director of Silent Talker, the company that developed the AI lie detection used in the iBorderCtrl-project)

Note that not all the resource persons mentioned above were available for an interview, and therefore not everyone mentioned above is part of the code labelling diagram in table 4. Dr. Patrick Breyer did respond to our request for an interview, but was unfortunately only able to answer written questions, which did not fit the form of our interviews. Therefore, he is not included in table 4.

3.2.1 Code labelling diagram

After completing the interviews, we transcribe the interview, analyse the interview and put their data in a code labelling diagram, which is a diagram that helps visualise what different resource persons have said about a topic. The code labelling diagram we have used can be seen in table 4. In the leftmost column, we have the name of the resource person, in the top row, we have the topics talked about; the cell at their intersection contains what the resource person said about that topic. This way, we can easily analyse what some of the recurring subjects are, which helps us identify areas of interest which we might research and ask other resource persons about.
Our analysis of the interviews consisted of the following steps:

1. Transcribe the interview
2. Identify topics mentioned in the interview
3. Add topics to the code labelling diagram if they are not yet in there, otherwise add them to the column of the relevant topic

After we conducted all the interviews, we focused on the topics that had been brought up multiple times by the interviewees. This we did by searching for all the topics that had more than one filled cell in their column, because this means that this topic has been discussed by more than one participant. Then, we made a version of the code labelling diagram which included only these topics, which can be seen as an "important topic"-list. This resulted in the code labelling diagram seen in section 7.

4 Theoretical framework

In this section, we elaborate on the theoretical framework that we will use in this thesis. This framework consists of the following three ethical theories: consequentialism, deontology and virtue ethics. Each theory will be explained in their own subsection.

4.1 Consequentialism

Consequentialism, as the name suggests, focuses on the consequences of an action to decide whether the action is good or not. If the consequences of an action are morally good, it means that the action itself is morally good. If they are not, the action is not morally permissible. Utilitarianism is probably the most famous form of consequentialism. A proponent of utilitarianism, like Jeremy Bentham, argues that the good action is the action that maximises the good, with the good being specified as pleasure and the absence of pain [Ben96]. Utilitarianism is a form of *act* consequentialism, since it focuses on the act itself and the consequences of that act. An alternative to this view is that of *rule* utilitarianism, which says that the moral rightness of an act depends on the consequences of a rule [Sin63]. Either form of consequentialism has the benefit that the application of the theory is fairly straightforward, since we can identify the consequences of applying a certain technology, and determining from there whether the application is morally permissible or not. An example of a simple application of consequentialism to technology is [Spa07, p. 67]. In our analysis, we will use an utilitarian framework, more specifically a form of act utilitarianism. We choose act utilitarianism, since we will be analysing a specific action – the applications of the technologies used in the iBorderCtrl-project – which means that act utilitarianism is the most logical choice.

4.2 Deontology

Deontology, which translates to "the study of duty", has a different way of determining whether an action is good. Instead of looking at the consequences of an action, deontology wants to know whether the action *in itself* is morally good or evil. A good way to illustrate the difference between deontology and consequentialism is that of lying. While a consequentialist might argue that lying in a situation is morally good since the consequences of that lie are good – the ends justify the means – a deontologist such as Kant argues that you can never lie, since it is morally forbidden for you to do so; there are no exceptions [Kan97]. Not all deontologists are as strict as Kant, but the notion of forbidden actions and inalienable rights is firmly part of the deontological tradition. This stems from the fact that respect for persons is a central concern of deontological ethics [Spa07]. Deontology gave us concepts like human rights, which play a central role in discussions about

technology and its application. We will therefore use a human rights framework in our deontological discussion of the technologies used in the iBorderCtrl-project.

4.3 Virtue ethics

Virtue ethics is different from the previous two theories discussed, in that it is agent-centered instead of action-centered. This means that the focus of virtue ethics lies on the person performing the action instead of the action itself. The central concept of virtue ethics is that of the moral virtue. From Aristotle onward, virtue has been understood in the Western tradition as a moral excellence that is part of one character, which we are not born with, but that must be cultivated in us [Ari84, 1103a20-35]. Since a historical account of the virtues, like that of Aristotle, does not account for new ethical questions that have emerged since the development of new technologies [Mac07], we will use a more contemporary view of virtue ethics. More specifically, we will use the formulation of virtue ethics of [Val16]. Vallor formulates her twelve virtues in response to what she calls a "acute sociotechnical opacity" [Val16, p. 6] in the 21st century, which means that "the practical circumstances of our everyday lives are changing so rapidly due to technological innovations that we cannot reasonably anticipate the impact of future states of affairs on our morality" [Rei19, p. E–18]. The twelve virtues that she identifies, and their meaning, can be found in table 2.

Virtue	Definition
Honesty	An exemplary respect for truth, along with the practical expertise to express that respect appropriately in technosocial contexts
Self-Control	An exemplary ability in technosocial contexts to choose, and ideally to desire for their own sakes, those goods and experiences that most contribute to contemporary and future human flourishing
Humility	A recognition of the real limits of our technosocial knowledge and ability; reverence and wonder at the universe's retained power to surprise and confound us; and renunciation of the blind faith that new technologies inevitably lead to human mastery and control of our environment
Justice	Reliable disposition to seek a fair and equitable distribution of the benefits and risks of emerging technologies & characteristic concern for how emerging technologies impact basic rights, dignity, or welfare of individuals and groups
Courage	Reliable disposition toward intelligent fear and hope with respect to the moral and material dangers and opportunities presented by emerging technologies
Empathy	Cultivated openness to being morally moved to caring action by the emotions of other members of our technosocial world
Care	Skilful, attentive, responsible, and emotionally responsive disposition to personally meet the needs of those with whom we share our technosocial environment
Civility	Sincere disposition to live well with one's fellow citizens of a globally networked information society; to collectively and wisely deliberate about matters of local, national and global polity and political action; to communicate, entertain, and defend our distinct conceptions of the good life; and to work cooperatively toward those goods of technosocial life that we seek and expect to share with others
Flexibility	Reliable and skilful disposition to modulate action, belief, and feeling as called for by novel, unpredictable, frustrating, or unstable technosocial conditions
Perspective	Reliable disposition to attend to, discern, and understand moral phenomena as meaningful parts of a moral whole
Magnanimity	Having a sense of nobility and self-worth founded in a life-time of moral and social efforts
Technomoral Wisdom	General condition of well-cultivated and integrated moral expertise that expresses successfully – and in an intelligent, informed, and authentic way – each of the other technomoral virtues

Table 2: The twelve technomoral virtues as identified by Vallor in [Val16]

5 Technologies used in the iBorderCtrl-project

In this section, we will take a high-level view of some of the technologies used in the iBorderCtrl-project, and their reliability. We will talk about the AI lie detection or Automatic Deception Detection System (ADDS) in a bit more detail, since this technology in particular was brought up multiple times in the interviews of section 7.

Term iBorderCtrl	**Generic term**	**Use of technology**
Biometrics Module	Fingerprint and palm vein technology	Scans traveller's fingerprints and palm veins to verify their identity
Face Matching Tool (FMT)	Facial recognition	Scans traveller's face to verify their identity
Document Authenticity Analytics Tool (DAAT)	Document verification	Used to check whether documents provided are legitimate
Hidden Human Detection Tool (HHD)	Radar and acoustic sensors	Detect people hidden in cars, trucks or trains
External Legacy and Social interfaces system (ELSI)	Information exchange interface	Check traveller data from SIS II (IT system for the exchange of information on people and object)
Risk Based Assessment Tool (RBAT)	Risk calculation	Calculates risk of fraud and other irregularities for every traveller
Integrated Border Control Analytics Tool (BCAT)	Analytics	Generates graphs and analytics about the performance of the iBorderCtrl systems
Automatic Deception Detection System (ADDS)	AI lie detection	Uses a traveller's webcam to scan their face to determine whether they are lying

Table 3: Inventory of all the technologies used by the iBorderCtrl-project [iBo21]

The iBorderCtrl-project encompassed a multitude of different technologies, which can be seen in table 3. To take just a small subset, these include: facial recognition, palm vein technologies, AI lie detection, and hidden human detection [iBo]. In this short discussion, we will talk about facial recognition and AI lie detection. The choice for focusing on these technologies was inspired by our selection criteria, which are societal impact and controversy. The facial recognition and AI lie detection are the technologies objected to the most by the interviewees in section 7, which fulfils our controversy criterion. Moreover, the possible impact of these technologies used in public spaces is large, which fulfils our societal impact criterion.
A further benefit of discussing these technologies in tandem is that the application of these two technologies is closely linked, which means that explaining one of these technologies enables us to better understand the other technology as well. We will start with a discussion of facial recognition and its reliability, and after that we will discuss AI lie detection.
Unfortunately, we do not know whether all of the technologies mentioned in table 3 were regularly used, or only incidentally. However [iBo21] gives us the impression of a tightly integrated system, in which each of these technologies exists in synergy with the others. This might indicate that all of these technologies should be operational at the same time. Therefore, we can conclude that all of these technologies were regularly used.

5.1 Facial recognition

5.1.1 Technical specification

Traditional facial recognition algorithms rely on two-dimensional images to recognise faces [LJ11]. The iBorderCtrl-project did not publish any specifications about what sort of facial recognition algorithm they are using. However, from the fact that the interview with the digital avatar can be conducted using a webcam, and taking into account that most webcams as of the moment of writing are not able to capture three-dimensional images, we assume that the iBorderCtrl-project used a two-dimensional facial recognition algorithm.
Traditional two-dimensional facial recognition is composed of four steps, namely

1. Face detection
2. Alignment
3. Establishing a feature vector of the face
4. Matching this feature vector against a database of faces [LJ11]

The processing flow of these four steps is visualised in figure 1.

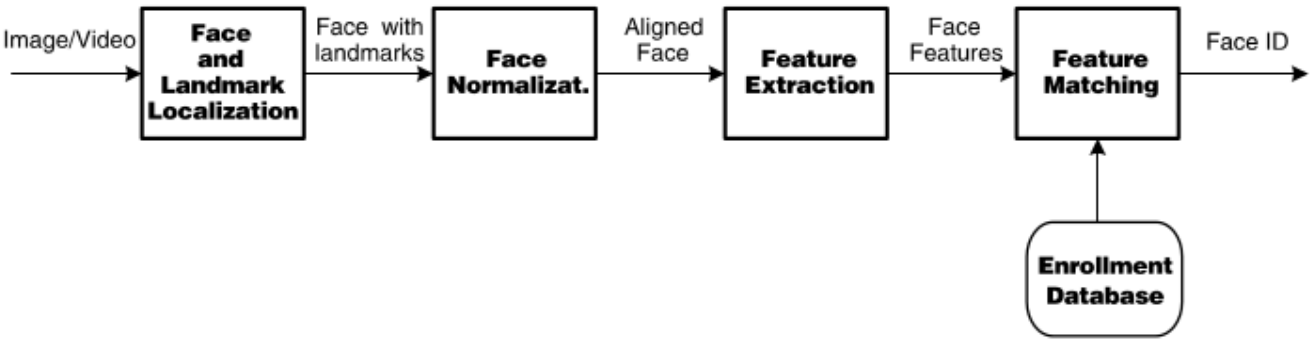

Figure 1: The four steps of facial recognition algorithms, as visualised by [LJ11, p. 4]

Face detection The first step in facial recognition is face detection. The goal of face detection is to locate and identify all the faces in a single picture, while not being hindered by differences in age, expression, orientation or lighting conditions [LJ11, p. 277]. The most widely used techniques go through the whole image using a subwindow, which is a small rectangle that looks at a part of the image. The algorithm then looks as the pattern in this subwindow, and classifies it either as a face or as a non-face. This is done for all the sections of the image, with differences in the sizes of the subwindow. The classifier (algorithm that classifies) used to distinguish faces and non-faces uses statistical learning methods to make the classification [LJ11, p. 277].

Alignment The second step in facial recognition is the alignment step. In this step, the image of the face that was detected in the first step is aligned to take into account the face pose and image details, for example, whether the image is grayscale or not [LJ11, p. 4].

Establishing a feature vector of the face After the image of the face has been aligned, it is possible to find features such as eyes, nose, jaw, mouth and cheekbone. These features are put into a feature vector of the face, which is a vector that contains all the information about these features. This feature vector is used for the face matching in the fourth step of the facial recognition algorithm [LJ11, p. 4].

Matching feature vector against a database of faces Finally, the feature vector is compared with one or multiple faces in the database of faces. If it matches with a face in the database, the algorithm gives "yes" as an output, to indicate that a match has been found. When comparing the feature vector with multiple faces, the faces in the database that match the feature vector the most are returned [LJ11, p. 4].

5.1.2 Reliability and accuracy

Over the last years, the accuracy (how many faces the algorithm can correctly identify) of facial recognition algorithms has improved somewhat. However, the accuracy of different algorithms still differs widely, even under ideal conditions. Research conducted by the National Institute of Standards and Technology (NIST) showed this difference in capability by researching the false negative identification rates[1] of different algorithms. This can be seen in the following excerpt of their report:
"Four algorithms miss more than 90% of subjects at NFP(T)[2] = 10, while nineteen algorithms achieve an FNIR below 25%, eleven achieve an FNIR below 15% at the same decision threshold, and five achieve an FNIR below 10% (M30V, M31V, M32V, G31V, G32V). On this basis, the marketplace capability is not broad." [GQN17, p. 35]
Furthermore, findings by multiple research groups indicate that most facial recognition algorithms suffer from higher false positive rates for people from Asian and African descent, especially for females of African descent [GQN17] [BG18]. Faces classified in NIST's database as African or Asian were 10 to a 100 times more likely to be misidentified than those classified as white [GQN17]. These results are especially relevant for our discussion of the iBorderCtrl-project, since an official adaption by border guards would mean that the technologies of iBorderCtrl would presumably be used on immigrants, which are for the most part minority groups like those which yield high false positive rates in the studies cited above.

5.2 AI lie detection

5.2.1 Technical specification

While the exact specifications about the AI lie detection system used by the iBorderCtrl-project remain vague, it is clear that their system relied on so called "micro-expressions", a concept first reported by Haggard and Isaacs [HI66], and expanded upon by Paul Ekman. Micro-expressions are facial expressions which are so short-lived, typically between 2/3 of a second and 4 seconds [EF82], that they remain mostly undetected by normal human eyes [HI66]. According to Ekman, these

[1] Type II error rate. A type II error is made when the null hypothesis is not rejected when it should be rejected
[2] Authors note: NFP indicates the fixed number of false positives, with T representing the fixed number

micro-expressions "leak" information about our true mental state [Ekm03], which means that we can use these micro-expressions to get information about someone's mental state.
The AI lie detection system used by the iBorderCtrl-project utilised the research about micro-expressions to determine whether the traveller wishing to cross the EU border is telling the truth while talking to the digital avatar. This technology is connected with the facial recognition technology discussed in section 5.1, since a face has to be detected before the AI lie detection system can look for micro-expressions. After detection of the face, the AI lie detection system "assumes that certain mental states associated with deceptive behaviours will drive an interviewee's [non-verbal behaviour] when deceiving" [OCK+18]. By looking at this non-verbal behaviour, the iBorderCtrl-project claimed to be able to spot deception.

5.2.2 Reliability and accuracy

The reliability and accuracy of lie detection in general, and AI lie detection in particular, has not been proven by the scientific research done in these fields. For example, Ekman's work on micro-expressions has been largely discredited [BJU07], and other research done on this topic has not been done according to the relevant scientific standards. This is the reason why Ekman's work is poorly regarded in the scientific and legal communities. Even Ekman himself recognises that there is no single indicator that tells us if somebody is lying, when he says: "We don't have something that only occurs when people are lying." [AK20]
Furthermore, even traditional lie detection methods, like the lie detection machine, have not shown to have scientific grounding as a device for establishing whether a subject is lying or not. In their research the National Academy of Sciences concluded that lie detection machines should not be used in court, since there is no scientific evidence for these machines [CN03]. In this same report, the National Academy of Sciences posited some questions that needed to be answered before a lie detection test could be seen as scientifically valid [CN03]. iBorderCtrl leaves most of these questions unanswered, and it seems likely that the webcams and smartphone-cameras, which are used to conduct the interview with the digital avatar, will not produce standardised measurements, which is one of the criteria for scientific validity introduced by the National Academy of Sciences.
Even if they exist, it is not clear if the AI lie detection system of iBorderCtrl will be able to detect micro-expression at all. Seminal research done on automatically analysing spontaneous micro-expressions report fairly low accuracy rates, ranging from 58.45%-65.55% for micro-expression detection, to 35.21%-52.11% for micro-expression recognition [LPH+13]. This research was done by, among others, a Research Lead at Google Cloud AI [Pfi21]. When even industry-leading experts report relatively low accuracy rates, it seems safe to assume that the iBorderCtrl-project, with its small budget compared to Google, had even lower accuracy rates. However, since iBorderCtrl has not published the accuracy rates of their AI lie detection system, this remains only a conjecture.

6 Applications of the technologies used in the iBorderCtrl-project

In this section, we will discuss some of the applications of the technologies used in the iBorderCtrl-project. We will do this based on the information provided by both the project itself, and by secondary sources, namely newspaper articles and other reporting. We will focus on the technologies discussed in section 5, since both facial recognition and AI lie detection play an important role in the application of the technologies of the iBorderCtrl-project.
The facial recognition and AI lie detection systems discussed in section 5 are both crucial to the avatar interview that is part of the pre-travel stage of the iBorderCtrl border crossing procedure [iBo]. Before this interview is conducted, prospective travellers to the European Union are asked to provide the following information [iBo]:

- Every country he/she will visit (length of stay, purpose of trip, expected date of arrival)
- Which travel documents he/she will use in each country
- A photo snapshot of aforementioned travel documents
- License plate, ownership documents, driver licence number
- A photo snapshot of the driver's licence

After this information has been checked for authenticity and has been stored in the iBorderCtrl-database, the traveller will talk to the digital avatar of a border guard.

6.1 Avatar interview

In this interview, prospective travellers will talk to a digital avatar of a border guard, which will ask them questions about themselves and their trip [iBo]. The avatar can be seen in figure 2. According to the iBorderCtrl-project, the questions that the avatar asks will be similar to questions asked by a real border guard [iBo]. These are not further specified, but they might include questions like: "What is the purpose of your trip?", "Where will you be staying?" and "How long do you intend to stay?" Before answering these questions, travellers will be asked to turn on their webcam. This is necessary, since their face needs to be visible for the AI lie detection and the facial recognition components to work.
While answering the questions of the digital avatar, the face of prospective travellers will be scanned by what the iBorderCtrl-project called the "Automatic Deception Detection System (ADDS)". This system is their version of AI lie detection. Since Automatic Deception Detection System is quite an opaque and verbose term, we will use the term AI lie detection for the remainder of this section. The working of the lie detection system are elaborated on by the project as follow: "The avatar interview is designed to detect false answers as it observes non-verbal behaviour. This means that the traveller will be filmed using his/her video camera while computer software observes facial (micro) gestures of the participant to detect deceptive behaviour." [iBo] The "facial (micro) gestures" referred to are the micro-expressions which are described by Ekman [EF82] [Ekm03].
After the interview has been completed, facial recognition is used to detect a face in the recorded video of the interview, and compare that face with the face on the prospective traveller's passport [iBo]. Since the only purpose here is to verify whether the traveller is actually who they say they are, we are dealing with facial recognition used for verification.

Figure 2: The digital avatar of a border guard the iBorderCtrl-project uses

7 Interviews with resource persons

In this section we will discuss the code labelling diagram we have constructed based on our interviews with the resource persons. This diagram can be seen in 4. Note that not all the resource persons mentioned in section 3.2.1 were available for an interview, and therefore not everyone mentioned there is part of the code labelling diagram in table 4. As mentioned in section 3.2.1, we have used a process whereby we first note all the topics discussed in an interview, and afterwards merge all the relevant topics. This way, we can identify the common issues raised by the resource persons, to better understand the iBorderCtrl-project and their perception of the project. We have only included the people who we have actually been able to interview, which means that not all the people mentioned in section 3.2 have been included. For brevity's sake, we also decided to only include the topics that have been mentioned by at least three resource persons. These topics are:

- Prominence of efficiency at the border
- Non-transparency issue
- Issues with lie detection
- Human rights framework

The topics have been formulated broadly by design, to allow for the greatest generalisation power possible. This means that different resource persons might stress different aspects of the topic, but that at the core all of them are talking about the same subject. How each resource person chooses to interpret that topic can be seen in table 4.
Since we have only included topics that have been discussed by at least three resource persons, a number of topics are omitted in table 4. For completeness' sake, we include them in the following list:

- Biometric data
- Article 22 of the GDPR
- Regulation of technology
- Security-industrial complex
- Using algorithms to find bias in border guards
- Biased algorithms
- Primary-secondary model
- Procedures and oversight
- Ethics/science whitewashing

Interviews	**Prominence of efficiency at the border**	**Non-transparency issue**	**Issues with lie detection**	**Human rights framework**
2021-02-02: Dr. Vera Wilde & Rop Gonggrijp	"I hope you will problematize, if you can the way that our focus gets drawn to policing borders better and more efficiently here, and of course, as a philosopher, is that something that we should be doing? What values should we be prioritizing?" [...] "When you look at how European non-Schengen borders are being policed in the water, it's, you know, Seawatch vs Frontex, running their drones, and one team is watching people die, and the other team is trying to save them. Maybe the drones are nice and efficient, but that is really not what Frontex should be doing."	"So, as science, it does not have a good standing in the scientific community, because the evidence-base is limited, and the evidence is mixed, and there's insufficient scientific evidence to say we should rely on this for any sort of decisions. But it was also totally non-transparent what they were actually doing [...] interview and talk to Dr. James O'Shea at Manchester Metropolitan University [...] waved his hands in the interview [...] and said: "Well, the great thing about our technology, is that we don't know what it's doing, we just train it to get the answers right, and then it does it, woohoo!" And that's not how this is supposed to work, right? That's a bad theory."	"Ekman's work has been mostly discredited in terms of assuming universality of seven basic emotions. So, as science, it does not have a good standing in the scientific community, because the evidence-base is limited, and the evidence is mixed, and there's insufficient scientific evidence to say we should rely on this for any sort of decisions" [...] "The text that explains to you why lie detection is pseudoscience, and why it is evil and bad." [...] "Vera could say: yes, this is pseudoscience."	"I think this is at the foundation of human rights, of freedom of thought, of association, the other, what we think of civil rights and civil liberties in the U.S., that you think more in terms of the declaration of human rights framework in Europe; if you do not protect the internal freedom of thought, if you do not protect cognitive liberty, then I think you are failing to protect the necessary conditions for freedom of thought."

2021-02-08: Dr. Petra Molnar	"[...] why are we using these tools when we know that: A. they don't work, B. they are human rights infringing, C. they are actually making the system less efficient because, guess what, people are going to start suing you. There is nothing as inefficient as lawsuits based on human rights, seriously. I mean, this efficiency argument, I think it doesn't hold any water, because it is not actually about efficiency, it's about, like, specific use of state power against people. If you really cared about efficiency, you would hire a lot more immigration officers, you would properly train them. You would set up courts, you would set up tribunals. So it's not about efficiency."	"For me, it been a kind of very instructive, useful example as well, because a lot of things that happen in this space are opaque and murky and difficult to, kind of, pin down [...] we know that the private sector is so based in, when it comes to, again, agenda-setting, priority-setting and just kind of creating this kind of opaque space where anything goes."	"Those traditional lie-detector, you know, the ones that go back-and-forth with the little arm, like the pictures, they're not even admissible in certain jurisdictions as evidence. Like, you can't bring that into a case, so why are we developing new lie-detectors when we know the old ones don't work anyway? It's like, dumb science, right?"	"In my work, you know, I use the human rights, kind of international human rights framework to try and show how far-reaching the impact of the migration management technology "panopticon" if you will, is. And again, the iBorderCtrl-project, the way that it was talked about, the way that it was developed, it really, really shows just how far-reaching the human rights ramifications of something like this could be."

2021-04-23: Dr. Matthew Longo	"Efficiency is not a value. The only value is justice. Every other thing that you're talking about, if it cuts into justice, it's no value at all. And so the problem is that efficiency, look, great, be efficient, if you're already just. The problem is that efficiency cuts into justice, it trades off on justice. And so they end of cutting corners for the sake of efficiency, that's the problem, right? So it's not efficiency or non-effiency, it's efficiency over and above very important things, that are basically the moral values we care about. [...] Anytime efficiency is the primary goal of any of these organisations, there's a big problem."			

2021-06-23: Konstantinos Kakavoulis	"I mean, efficiency is not a bad thing, unless it's the only priority. We should just balance with all the [...] As I've said before, they should always be aware and try to respect the legal and ethical issues around all this. " [...] "So we should not say that, in order to capture and condemn all criminals going around the European Union, it is okay to also capture and condemn a few innocent citizens. This is not how the Western philosophy for law operates. The Western philosophy for law clearly says that everybody is innocent until it is proven the other way. So, we should always keep this in mind, and we should not, in the name of efficiency, and in the name of keeping Europe a more secure place than others, go against the philosophy with which our Western legislation, but also civilization has been created. "	"It's at least strange to say that all of these reports are confidential, and at least something should have been made public, or at least disclosed to anyone having an legitimate interest to request. And since we have requested it, at least receive a part of these reports" [...] "If the opinion has been granted, and if they have found that everything is lawful, than why not make it publicly available? I can understand that some part of the data protection impact assessment can not be publicly available, maybe they should be treated as confidential because they have to do with the technical security of the software, but this does not mean that the data protection impact assessment as a whole, or at least most parts of it, should not be available"	"We cannot understand how with so few money you can get such a good lie detection AI software. And our greatest concern is what happens with false positives."	"Yeah, so apart from all the privacy issues that we have discussed before, it is also a very important issue that there is a human rights impact assessment as well. So, this is why we have asked for the ethical reports on the project." [...] "We definitely believe that this is the way forward, but we should just not rush that much, so that people's rights are also respected. We definitely believe that in the coming years we're going to have more and more technology being implemented, and we're not against this, but we definitely are asking for more transparency and more legal regulation of this technology use. As well as better implementation of this framework. So, not just that this legal framework exists, but also that it is taken into account when designing new projects."

Table 4: Code labeling diagram

8 Analysis of the iBorderCtrl-project using three different ethical theories

In this section, we will analyse the applications of the technologies specified in section 6, using the theoretical framework we outlined in section 4. For clarity, we will discuss each ethical analysis in a separate subsection, using the same order as used in section 4.

8.1 Consequentialism

As mentioned in section 4.1, we will use a form of act utilitarianism to analyse the applications of the technologies of the iBorderCtrl-project. We will focus on the two main groups involved in a border crossing, namely travellers and border guards.

8.1.1 Travellers

We can identify multiple negative consequences for travellers of the application of the technologies in the iBorderCtrl-project.

Bias First of all, travellers will probably be discriminated against by the AI lie detection system. This has two reasons; a general reason and a specific reason. The general reason is that AI systems in general tend to substantiate existing human biases towards minority groups [KvP11] [MAT+16]. Furthermore, as mentioned in section 5.1.2, facial recognition contains a racial bias to lighter skin colours [BG18]. Since most non-EU travellers will belong to a minority group and/or have a darker skin colour, this bias and the discrimination that follows will harm them.
The specific reason why the technologies used in the iBorderCtrl-project are problematic for the traveller, is that they have been trained on a very limited training set, with only 32 people, that contained twice as much men as women, and no Hispanic or black people [OCK+18] [Bit20]. This very small and homogeneous training set means that the system will probably be very biased towards white men, worsening the bias that these systems already suffer from in themselves. This increased bias means that the harm suffered by a non-white, non-EU traveller will be even greater than mentioned above.

Psychological harm While not all utilitarians agree about whether psychological harm constitutes "real" harm, the added psychological harm to potentially already traumatised travellers is too important to overlook. Therefore, we will include psychological harm in our consequentialist analysis. This psychological harm is twofold.
First of all, being discriminated against may result in feeling inferior, and developing an inferiority complex [Wil99]. This inferiority complex is a feeling of inadequacy, which often results in the belief that one is somehow inferior to others [EAJ17]. While the one interaction with the technologies of the iBorderCtrl-project will not immediately make travellers develop an inferiority complex, the discrimination by the AI lie detection system and possibly also by the human border guard will further entrench any existing feelings of inferiority they may have. This has grave consequences for the further lives of the travellers, since an inferiority complex is linked to worse study and work results [Hut07], and overall reduced levels of happiness [AC19].

Another factor that might hurt the self-esteem of the travellers, is the implicit assumption behind the AI lie detection system, namely, that all the non-EU travellers who are trying to get into the EU will be lying, or will at least be inclined to lie. Being in this position, where you are asked to "prove" that you are not lying by being subjected to an interview, is very degrading. Even if this does not lead to the development or worsening of an inferiority complex, the consequences of being degraded are by themselves grave enough to constitute psychological harm.

8.1.2 Human border guards

The consequences for human border guards will be mostly good, since the use of the technologies seems to have been designed with their interests in mind.
The biggest benefit of using these technologies for the border guards is that it makes the process of border crossings more efficient from their point of view. This is explicitly stated in one of the press releases of the European Commission: "the project is aiming to deliver more efficient and secure land border crossings to facilitate the work of border guards" [Eur18]. The amount of work taken out of the hands of the human border guards is perfectly illustrated in the following passage from the press release:
"Border officials will use a hand-held device to automatically cross-check information, comparing the facial images captured during the pre-screening stage to passports and photos taken on previous border crossings. After the traveller's documents have been reassessed, and fingerprinting, palm vein scanning and face matching have been carried out, the potential risk posed by the traveller will be recalculated. Only then does a border guard take over from the automated system." [Eur18].
Apart from the learning curve of these technologies, the amount of direct negative consequences for the human border guards will probably be very limited. However, we could identify a possible future consequence of the iBorderCtrl-project, namely automation of the jobs currently done by human border guards. According to [Bal19] mid-qualification jobs will most likely be automated in the near future. Since being a border guard is a mid-qualification job, it seems likely that a successful pilot of the iBorderCtrl-project would lead to increasing interest in the possibility of automating this. Therefore, one of the possible negative consequences of the iBorderCtrl-project for the border guards is the fact that their jobs might disappear in the future if this project is successful. However, since it is unclear how fast the development of these technologies will go, it might not be on the human border guards' minds that this is a possibility.

Conclusion For brevity's sake, we have chosen to focus on two main groups involved in border crossings in our consequentialist analysis of the technologies used in the iBorderCtrl-project. We saw that the consequences for travellers are very negative and very serious, while the benefits for human border guards are relatively minor. Therefore, our utilitarian calculus is relatively clear: very negative consequences for a majority (the travellers) versus minor positive consequences for a minority (the human border guards) leads us to the conclusion that the application of the technologies used in the iBorderCtrl-project is more ethically condemnable in a consequentialist sense.

8.2 Deontology

Many of our modern rights-based perspectives of morality are based on deontology. As mentioned in section 4.2, respect for persons is the central concern of deontological ethics. This respect for persons and their inalienable rights, especially in the Kantian sense, is what lies at the foundation of our modern conception of human rights [Ore00, p. 90].
For our deontological analysis, we will use a human rights framework to access the project. This has two reasons: firstly, the aforementioned deontological nature of human rights, and secondly, the fact that the human rights framework was mentioned often in the interviews conducted with resource persons, as seen in section 7. Since the complicated nature of border crossings makes legal questions about which laws apply a bit murky, we will use the framework that by it's very nature applies to every human being, namely the Universal Declaration of Human Rights [Uni48]. The human rights that we will use in our discussion are:

- Dignity (Article 1)
- Right to privacy (Article 12)
- Freedom of thought, religion and conscience (Article 18)

It is important to note that for a deontologist these rights always apply, and are therefore above any considerations about efficiency and practical implementation of a system. Therefore, the efficiency argument will not be discussed in this section, since it is not relevant to a deontologist analysis. This is eloquently expressed by Dr. Matthew Longo in his interview:

"Efficiency is not a value. The only value is justice. Every other thing that you're talking about, if it cuts into justice, it's no value at all."

Right to privacy It is clear that some boundary has been overstepped by the technologies of the iBorderCtrl-project. However, it is still difficult to argue that the invasion of privacy in the iBorderCtrl-project is entirely arbitrary, which is article 12 explicitly mentions: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation." [Uni48] The invasion cannot be seen as entirely arbitrary, because the state has granted a lot of power to border guards to examine everyone who crosses the border, so this invasion of privacy is not entirely arbitrary. In this situation, the GDPR might help us to understand clearly what should be seen as arbitrary. One of the foundational principles of the GDPR is that of data minimisation: you only should collect and process personal data that is absolutely necessary to fulfil your purpose. This is clearly not the case in the iBorderCtrl-project, so therefore we can argue that the right to privacy of the travellers has been violated by the technologies used in the iBorderCtrl-project.

Right to freedom of thought and conscience One of the biggest issues with lie detection is that it aims to learn what our inner emotional state is by looking at outward appearances. As mentioned in section 5.2.2, it is not entirely clear that this actually works. However, whether it works or not is beside the point, we will look at whether the intention itself is in violation with the right of thought and conscience.
As mentioned in section 5.2.2, the AI lie detection uses micro-expressions to get information about someone's mental state. This information of a mental state is then used to determine whether

someone is lying or not. However, we can argue that this goal of trying to guess someone's mental state is in itself a violation of the right to freedom of conscience. [Far18] argues for a so-called "right to cognitive liberty", a sort of mental privacy right that makes it impossible for states and other actors to read your mental state. If this right existed already, it would clearly be violated by the AI lie detection. However, arguably this right to cognitive liberty is already captured by the freedom of thought, as Dr. Vera Wilde expresses in her interview: "if you do not protect the internal freedom of thought, if you do not protect cognitive liberty, then I think you are failing to protect the necessary conditions for freedom of thought" Regardless of whether the right to cognitive liberty is captured by the freedom of thought already, the concept does provide us with a useful way to think about the human right to freedom of thought and conscience, since it allows us to characterise a mental state as a thought. Building on this idea, we can say that the attempt to guess someone's emotional state by using AI lie detection is violating the traveller's right to freedom of thought and conscience.

Dignity To go back on a more Kantian perspective, the interview with the digital border guard and the accompanying AI lie detection is degrading for a human being. It does not see the humanity in the human being, which is a central concept (we follow [Hil19] in this interpretation) in Kant's second formulation of the Categorical Imperative: Act in such a way that you always treat humanity, whether in your own person or in the person of any other, never simply as a means but always at the same time as an end" [KTG11]
The interview with the digital border guard is harmful to human dignity, because it indicates that the traveller is not worth the time of an actual border guard, and will therefore have to be subjected to an interview by a computer. This is harmful to the fundamental right of dignity set out by [Uni48]. Therefore, this right to dignity is among the rights that were violated in the iBorderCtrl-project.

Conclusion In our deontological analysis of the application of the technologies used in the iBorderCtrl-project, we have seen that many of the human rights set forth in [Uni48] have been violated. Among the rights that are most gravely affected are the right to privacy, the right to freedom of thought and conscience, and the right to dignity. Following Kant and the larger deontological tradition that says that these rights may never be violated, we conclude that the fact that they have been violated by the iBorderCtrl-project means that deontology would see this project as immoral. Konstaninos Kakavoulis, of the Greek digital rights organisation Homo Digitalis, agrees: "We definitely believe that this is the way forward, but we should not rush that much, so that people's rights are also respected."

8.3 Virtue ethics

Many different values and virtues are prioritised at the border, but are these values and virtues the ones that we should be expressing, or should we realign our values? Dr. Vera Wilde summarises the issue in an eloquent was: "Our focus gets drawn to policing borders better and more efficiently here, and of course, as a philosopher, is that something that we should be doing? What values should we be prioritizing?" The central question we will discuss in our virtue ethics-analysis is the following: "How are the applications of the technologies used in the iBorderCtrl-project shaping

human habits, skills, and traits of character for the better, or for the worse?"[3]. We will do this by looking at the impact of these technologies on the technomoral virtues listed in table 2. We will focus on the two central kinds of agents at the border: the traveller, and the border guard, and see what the answer is for them.

8.3.1 Traveller

Humility A traveller's interaction with the technologies of the iBorderCtrl will help them foster the technomoral virtue of humility. They will be confronted by a faulty system that has been trained on only a few examples, and tested by the same researchers that created the system [Bit20]. This will make it clear to them that technology is not infallible, and that blind faith in this technology, as expressed by some of the developers of the iBorderCtrl-project [Bit20], is unfounded. This increased awareness of the limits of technology will make the traveller renounce the any blind faith they have left that new technologies inevitably lead to human mastery and control of our environment; therefore, the application of the technologies used in the iBorderCtrl-project will positively impact the humility of travellers.

Justice A traveller's sense of justice and the ability to express this will be negatively affected by the technologies of the iBorderCtrl-project, since it will make clear that justice is not valued at the border. This lessens the value of justice in the traveller's eyes, since it indicates that society, and in particular European society, does not concern itself with how these technologies impact the basic rights, dignity and welfare of the traveller. Having powerful institutions implicitly indicate that they do not care what is just, that they only care about what is efficient for themselves, is detrimental to the value of justice in the traveller's eyes. While travellers may feel they are being unfairly treated, and therefore are able to understand the value of justice all the better, their treatment by the iBorderCtrl-project will teach them that justice is not a virtue worth having. This might make them disinclined to foster the habit of justice in themselves. Therefore, the application of the technologies used in the iBorderCtrl-project will negatively impact the justice of travellers.

Courage The traveller's ability to express courage might be both positively or negatively impacted by the technologies used in the iBorderCtrl-project.
On the one hand, travellers' interaction with these technologies might make them more aware of the moral and material dangers of these technologies, since they themselves have now experienced the negative consequences. According to Dr. Petra Molnar, the people impacted by these technologies have very clear opinions about them: "I talk to refugees, I talk to people at the border, they have really really strong opinions about things. They might not be able to talk about, I don't know, binary code or whatever, but they sure as hell can talk about systemic racism and how it's perpetuated by technology." This might contribute to building what [Val16] calls "intelligent fear and hope" of these technologies. In this respect, experience of the technologies might contribute to a traveller's courage.
On the other hand, this technology might also negatively impact a traveller's courage. Having a very disagreeable experience with these technologies at the border, a traveller might stay away from other technology that positively benefits their lives, like using the internet to apply for governmental

[3]Inspired by [Val16, p. 211]

support. This general fear of technologies would negatively impact the traveller's ability to flourish, and would therefore be a negative effect on the traveller's courage, since the fear becomes too dominant in situations where hope for the opportunities of technologies would be more warranted.

Magnanimity Magnanimity will be greatly affected by the technologies of iBorderCtrl. Especially the interview with the digital avatar will have a negative effect on the traveller's sense of nobility or self-worth. Being subjected to this interview will make it clear to the traveller that they are not even worth the time of a human border guard, which is very degrading. Furthermore, the goal of the interview is to check if they were truthful when they submitted their documents. Therefore, there is an implicit assumption that all the traveller's are more disposed to lie on their applications. This is another way in which their self-worth will be harmed, since they have to prove that they are not lying, while EU citizens are not required to do this. This kind of two-tier system is degrading, since it indicates that the traveller is worth less and has to have different expectations than an EU citizen. Therefore, the application of the technologies used in the iBorderCtrl-project will negatively impact the magnanimity of travellers.

Conclusion On the whole, the applications of the technologies used in the iBorderCtrl-project shape the habits, skills and traits of character of the traveller for the worse. Humility, justice and magnanimity are among the virtues that will be particularly impacted. Therefore, the application of these technologies will make it more difficult for a traveller to flourish as a human being.

8.3.2 Human border guard

Humility The use of AI lie detection and facial recognition through the digital avatar of a border guard will probably make it more difficult for a human border guard to express humility. Since the goal of the iBorderCtrl-project is to make border crossing more efficient, the human border guard will probably become very reliant on the judgement of the digital avatar, since going against that judgement would take more time, which is inefficient. We have seen this reliance in the United States, where judges were relying on a discriminatory algorithm that predicted recidivism [ALMK16]. According to [Rah19], this reliance on algorithms in US courtrooms is increasing.
We will assume that judges take more effort to come to a fair judgement than a typical border guard, since judges have been explicitly trained to hone their judgement to reach a fair decision [GRW01]. Furthermore, since the iBorderCtrl-project is being tested in countries that are only partly free, i.e Hungary [Fre20], there will probably be no institutional pressure for the human border guards to express humility about their own judgement and that of the algorithm. Therefore, the application of the technologies used in the iBorderCtrl-project will negatively impact the humility of human border guards.

Justice Justice is another techonomoral virtue that will probably suffer by using the technologies of iBorderCtrl. As we discussed in sections 5.1.2 and 5.2.2, there are many concerns about the fairness of these technologies. According to Dr. Petra Molnar, one of the resource persons interviewed for section 7, fairness might not even be a central concern when developing this technology: "I almost feel like these tools are not meant to work, they are to signal that the state has the power to decide who comes and goes, and now they have a fancy new tool to do it through." According to Molnar, these technologies are not used as a tool for justice, but as a signal of state power.

These tools, which do not encourage fair decisions and might just be there to be used as a signal, will disincentive human border guards to think about the impact that these technologies have on the basic rights, dignity and welfare of the travellers they have to "process". Therefore, the application of the technologies used in the iBorderCtrl-project will negatively impact the justice of human border guards.

Empathy By using these technologies as a sort of "digital wall" between themselves and the traveller, human border guards might become less empathetic, since their first impression of a traveller will be formed by the analysis given to them by the digital avatar. If this analysis is negative, the border guard will be poised to be negative about the traveller as well, thereby limiting the possibility of empathy. The technology used in the iBorderCtrl-project seems to have the purpose of widening the gap between border guard and traveller, by making their interaction mediated by technology. This means that the border guard will be less able to be morally moved to caring action, since the mediated interaction tries to remove as much of the emotion as possible. Therefore, the application of the technologies used in the iBorderCtrl-project will negatively impact the empathy of human border guards.

Flexibility It is not entirely clear how flexibility of human border guards will be affected by the technologies used in the iBorderCtrl-project. On the one hand, most of the border guards will have never used a system like this, which will lead to the need to improvise and adapt to new challenges when learning to work with the technology. These new challenges might help the border guards get out of their ingrained patterns, and re-evaluating these patterns based on the insights from the digital avatar.
On the other hand, these technologies have the potential to further entrench existing discriminatory practises, by making it easy for the border guard to justify their ingrained patterns, by pointing to the scepticism of the digital avatar about a traveller's motives. This digital avatar might reproduce existing patterns of discrimination, like many of the algorithms mentioned in [CS14]. Thus, the technologies might also make the human border guards less flexible, by reducing their willingness to change their actions and by further entrenching their existing patterns.

Conclusion On the whole, the applications of the technologies used in the iBorderCtrl-project shape the habits, skills and traits of character of the human border guard for the worse. Humility, justice and empathy are among the virtues that will be particularly impacted. Therefore, the application of these technologies will make it more difficult for a human border guard to flourish as a human being.

9 Conclusions and Further Research

9.1 Conclusions

We have investigated how the three ethical theories, namely consequentialism, deontology and virtue ethics, would analyse and judge the application of the technologies used in the iBorderCtrl-project. As can be expected with such different theories, their exact analysis of the project differs. However, each of the theories does ultimately deem the application of the technologies unethical. Consequentialism uses its calculus to find out that this application increases human suffering, and is therefore immoral. Deontology see a violation of inalienable human rights in the application of the technology, and draws its conclusion. Finally, virtue ethics concludes that the application of these technologies is a hindrance to human flourishing, and therefore see this application as immoral. Thus, we conclude that each of the three main ethical theories sees the application of facial recognition and AI lie detection as part of the iBorderCtrl-project as immoral.

9.2 Limitations

There are some limitations to our work, namely:

- The fact that we were not able to interview a very extensive group of resource persons, which might have been disadvantageous to our understanding of the project. In particular, we were not able to interview someone connected to the iBorderCtrl-project itself, since they did not respond to our request for an interview.
- Since we did an explorative study of the iBorderCtrl-project, we were not able to provide definite conclusions. This means that other researchers will need to do their own research, since they cannot consider our conclusions to be final.
- The study does not provide a clear argumentation for why certain theories were chosen above others

9.3 Further research

Further research in this area is needed to fill in gaps in our knowledge. Since applied ethics is a relatively novel field, there are not yet clear standards about how a ethical analysis of a project should be conducted. We think that our comparative approach, which shows the three main ethical theories side-by-side, has the potential to be valuable in thoroughly understanding situations where technological and moral questions intertwine. As paths for further research, we suggest the following:

- Exploration of the perception of the general public of projects like iBorderCtrl. To be valuable in a European context, this research would need to interview a representative group of Europeans to ensure that the results are not biased by citizenship of a certain country. Furthermore, the group needs to include a variety of views, so that different viewpoints can be taken into account and a more nuanced analysis can be provided.
- Development of novel ways in which the comparative analysis used by this thesis could be used in a more structured way, so that it can be used by policy makers to determine whether funding of a certain project or technologies is a good thing to do. This standard should be

structured enough to provide guidance, but flexible enough to still be useful in a wide variety of cases. Since each of the three ethical theories are very flexible, we believe that this is possible.

References

[AC19] Ramazan Akdogan and Elif Cimsir. Linking inferiority feelings to subjective happiness: Self-concealment and loneliness as serial mediators. *Personality and individual differences*, 149:14–20, 2019. Publisher: Elsevier Ltd.

[AK20] Jad Abumrad and Robert Krulwich. Deception. https://www.wnycstudios.org/podcasts/radiolab/episodes/91612-deception, November 2020. Online; accessed 2021-05-24.

[ALMK16] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner. Machine Bias. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, 05 2016. Online; accessed 2021-05-24.

[Ari84] Aristotele. *The Complete Works of Aristotle: the Revised Oxford Translation*. Bollingen series ; 71:2 811588971. Princeton University Press, Princeton ; Guildford, 1984.

[Bal19] Richard E Baldwin. *The Globotics Upheaval: Globalization, Robotics, and the Future of Work*. Oxford University Press, 2019.

[Ben96] Jeremy Bentham. *An Introduction to the Principles of Morals and Legislation*. The collected works of Jeremy Bentham. Clarendon Press, Oxford, [repr.] / with a new introd. by F. Rosen; and an interpretive essay by H.L.A. Hart. edition, 1996.

[BG18] Joy Buolamwini and Timnit Gebru. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *PMLR*, page 15, 2018.

[Bit20] Jake Bittle. Lie detectors have always been suspect. AI has made the problem worse. *MIT Technology Review*, 2020.

[BJU07] Charles F Bond Jr and Ahmet Uysal. On Lie Detection "Wizards". *Law and human behavior*, 31(1):109–115, 2007.

[CN03] Committee to Review the Scientific Evidence on the Polygraph (National Research Council (U.S.)) and National Research Council (U.S.). *The Polygraph and lie detection*. National Academies Press, Washington, D.C., 2003.

[CS14] Kate Crawford and Jason Schultz. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College law review*, 55(1):93, 2014.

[EAJ17] Richard M Elliott, Alfred Adler, and Jelliffe. Study of organ inferiority and its psychical compensation. a contribution to clinical medicine. *Journal of the American Institute of Criminal Law and Criminology*, 8(2):305–306, 1917.

[EF82] Paul Ekman and Wallace V Friesen. Felt, False, and Miserable smiles. *Journal of nonverbal behavior*, 6(4):238–252, 1982.

[Ekm03] Paul Ekman. Darwin, Deception, and Facial expression. *Annals of the New York Academy of Sciences*, 1000(1):205–221, 2003.

[Eur18] European Commission. Smart lie-detection system to tighten EU's busy borders. https://ec.europa.eu/research-and-innovation/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders, 10 2018. Online; accessed 2021-05-26.

[Far18] Nita Farahany. When technology can read minds, how will we protect our privacy? https://www.ted.com/talks/nita_farahany_when_technology_can_read_minds_how_will_we_protect_our_privacy, 11 2018. Online; accessed 2021-05-27.

[Fre20] Freedom House. Freedom in the world — Hungary country report. https://freedomhouse.org/country/hungary/freedom-world/2020, 05 2020. Online; accessed 2021-05-24.

[GQN17] Patrick J Grother, George W Quinn, and Mei Lee Ngan. Face in video evaluation (FIVE) face recognition of non-cooperative subjects. Technical Report NIST IR 8173, National Institute of Standards and Technology, Gaithersburg, MD, March 2017.

[GRW01] C Guthrie, JJ Rachlinski, and AJ Wistrich. Inside the judicial mind. *Cornell law review*, 86(4):777–830, 2001.

[HI66] Ernest A Haggard and Kenneth S Isaacs. Micromomentary facial expressions as indicators of ego mechanisms in psychotherapy. In *Methods of research in psychotherapy*, pages 154–165. Springer, 1966.

[Hil19] Thomas E. Hill. *Dignity and Practical Reason in Kant's Moral Theory*. Cornell University Press, 2019.

[Hut07] Guy K Hutt. *Experiential learning spaces: Hermetic transformational leadership for psychological safety, consciousness development and math anxiety related inferiority complex depotentiation*. ProQuest Dissertations Publishing, 2007.

[iBo] iBorderCtrl Project. *Letter of Informed Consent concerning the participation as a volunteer in the iBorderCtrl project*.

[iBo21] iBorderCtrl Consortium. iborderctrl. https://www.iborderctrl.eu/, 2021. Online; accessed 2021-06-15.

[Kan97] Immanuel Kant. On a Supposed Right to Tell Lies from Benevolent Motives, 1797.

[KTG11] Immanuel Kant, Jens Timmermann, and Mary Gregor. *Groundwork of the metaphysics of morals: a German-English edition*. Cambridge University Press, 2011.

[KvP11] U.A.F Kraemer, C.W.A.M van Overveld, and M.B Peterson. Is there an Ethics of Algorithms? *Ethics and information technology*, 13(3):251–260, 2011.

[LJ11] Stan Z. Li and Anil K. Jain. *Handbook of Face Recognition*. Springer-Verlag London, 2011.

[LPH+13] Xiaobai Li, Tomas Pfister, Xiaohua Huang, Guoying Zhao, and Matti Pietikainen. A Spontaneous Micro-expression Database: Inducement, collection and baseline. In *2013 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, pages 1–6, Shanghai, China, April 2013. IEEE.

[Mac07] Alasdair C. MacIntyre. *After Virtue : A Study in Moral Theory*. Notre Dame, Ind. : University of Notre Dame Press, 2007.

[MAT+16] Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, and Luciano Floridi. The Ethics of Algorithms: Mapping the debate. *Big data & society*, 3(2):205395171667967, 2016.

[OCK+18] James O'Shea, Keeley Crockett, Wasiq Khan, Philippos Kindynis, Athos Antoniades, and Georgios Boultadakis. Intelligent Deception Detection through Machine Based Interviewing. In *2018 International Joint Conference on Neural Networks (IJCNN)*, pages 1–8, 07 2018.

[O'N16] Cathy O'Neil. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. The Crown Publishing Group, 2016. Publication Title: Weapons of Math Destruction.

[Ore00] Brian Orend. *War and International Justice: A Kantian Perspective*. Wilfrid Laurier University Press, Waterloo, 2000. Publication Title: War and International Justice.

[Pfi21] Tomas Pfister. Tomas Pfister - Personal webpage. https://tomas.pfister.fi/, 2021. Online; accessed 2021-05-24.

[Rah19] Kia Rahnama. Science and Ethics of Algorithms in the courtroom. *Journal of law, technology & policy*, 2019(1):169, 2019.

[Rei19] Wessel Reijers. Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting by Shannon Vallor (review). *Kennedy Institute of Ethics journal*, 29(1):E–17–E–27, 2019. Place: Baltimore Publisher: Johns Hopkins University Press.

[SHLH21] Taylan Sen, Kurtis Haut, Denis Lomakin, and Ehsan Hoque. A Mental Trespass? Unveiling Truth, Exposing Thoughts and Threatening Civil Liberties with Non-Invasive AI Lie Detection. *CoRR*, abs/2102.08004:11, 2021.

[Sin63] Marcus G. Singer. *Generalization in Ethics : an Essay in the Logic of Ethics, with the Rudiments of a System of Moral Philosophy*. Eyre & Spottiswoode, London, 1963.

[Spa07] Robert Sparrow. Killer Robots. *Journal of Applied Philosophy*, 24(1):62–77, February 2007.

[Uni48] United Nations. Universal Declaration of Human Rights, December 1948.

[Val16] Shannon Vallor. *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting*. New York, NY : Oxford University Press, 2016.

[Wil99] David R. Williams. Race, Socioeconomic Status, and Health The Added Effects of Racism and Discrimination. *Annals of the New York Academy of Sciences*, 896(1):173–188, 1999. Place: Oxford, UK Publisher: Blackwell Publishing Ltd.