INTERNATIONALE HOCHSCHULE FERNSTUDIUM

Proposal for a regulation framework for facial recognition technology

Maximizing the benefits while minimizing the risks

Data Science and Society

(DLMDSSDSS01)

Niels Humbeck

32003045

23.12.2020

Halle (Saale)

1 Table of contents

2 Image directory

3 Abbreviations

AI	Artificial Intelligence
CSL	Cyber security law
MOST	Ministry of science and technology
NIST	National Institute of Standards and Technology

4 Introduction

Facial recognition technology are recently used for controlling the COVID 19 pandemic in different countries around the world. In Moscow facial recognition technology is used to control the quarantine of citizens since the beginning of the COVID 19 pandemic (Reevell, 2020). Facial recognition technology was combined with thermal imaging to detect persons with elevated temperatures (Natta, Herbek, 2020). This multimodal system was deployed for example in Thailand for border controls (Böckler, 2020) and in companies to track employees and visitors (Ramco, 2020). The deployment of facial recognition technology can be beneficial for an efficient pandemic control and thus beneficial for society. On the other side there are massive concerns about the use of facial recognition technology for induvial privacy rights as well as human and constitutional rights (e.g. Chun, 2020 or Natta, Herbek, 2020). In Germany the health authorities work with outdated technology like fax machines to control in an not efficient manner infection chains in this pandemic because of strong data protections laws (Schumacher, 2020).

This research assay propose a regulation framework for facial recognition technology to maximize the potential benefits of this new technology while minimizing or mitigating the risk arising from it. Chapter 5 describes the historical development of facial recognition technology, the capabilities and the working methods of modern facial recognition technology. The potential benefits deploying facial recognition technology as well as the potential arising risks to society are discussed in chapter 6. Before the here proposed regulation framework is discussed, the existing regulation frameworks in the jurisdictions USA, EU and China are explained in chapter 7. The jurisdictions USA, EU and China are chosen because these three areas are the main developing centers for artificial intelligence such as facial recognition technology. Finally a regulation framework for facial recognition technology is presented to enable the beneficial use of this new technology while mitigating and minimizing the risks to society arising with this technology in chapter 8. In Chapter 9 the conclusion of this research essay is discussed.

5 The development of Facial Recognition Technology

Woodrow Bledsoe the founder of the company Panoramic Research (Palo Alto, California 1965) is seen as the pioneer of facial recognition technology. Together with a researcher team he developed a database driven technology to match a face with faces stored in a database. He "[…] reduced a face to a set of relationships between its major landmarks: eyes, ears, nose, eyebrows, lips. The system that he imagined was similar to one that Alphonse Bertillon, the French criminologist who invented the modern mug shot, had pioneered in 1879" (Raviv, 2020). He called his invention a "man-machine". Since in 1965 the digital photography processing was not well-advanced, Mr. Bledsoe choose a two step approach. In the first step a human measures the relationship between major landmarks in a face on a photography and enter these distance ratios in a database. In the next step a computer matches the entered face with one of the stored face, which fits the best (Raviv, 2020). The prove of concept was performed.

Mr. Goldstein, Mr. Harmon and Mrs. Lesk did in the 1970s a comprehensive study to identify the most significant characteristics of a human face for identification purposes. They discovered that just 22 features "[…] provide relevant, distinctive, relatively independent measures which can be judged reliably". (Goldstein, Harmon and Lesk, p.748, 1971) This work improves the accuracy of the facial recognition technology significantly and reduces the processing time. Never the less it was not possible to perform the facial recognition task fully computer automated. The measurements still has to be taken by humankind. The breakthrough of the automated facial recognition technology came with the development of digital photography processing, as well as increasing data storage and processing capacities in the 90th and early 2000th. The theory of the first fully automated real-time facial recognition technology was developed Mr. Sirovich and Mr. Kirby (1987) and deployed by Turk and Pentland (1991): "The approach transforms face images into small set of characteristic feature images, called "eigenfaces", which are the principle component of the initial training set of face images." (Turk & Pentland, 1991, p.1) Basically the given pictures of 2-D-faces were reduced by using PCA (principle component analysis) to a 2-D-eigenface, which means a reduction in dimensionality. The eigenface shows the biggest variances in comparison to a calculated "mean" face of a given population. To recognize a person its eigenface is set as a linear combination of the stored eigenfaces. To identify the most likely matching eigenface in the database the k-neighbors algorithm is applied. This technology is scalable and the technology can be used in real time. A big disadvantage of this technology is that its really sensitive to light. Photography of faces from a video or a surveillance camera are not suitable for that technology since the angle of the head or the face expression differs to much resulting in lower accuracy rates (Turk & Pentland, 1991).

Around the turn of the century social networks like Facebook were invented. With increasing popularity the number of users as well as the number of uploaded photos increased significantly. Since it's a social network most photos contain faces leading to a huge database of faces. Facebook developed an facial recognition technology called DeepFace in 2015. DeepFace deploys a "deep neural net (DNN) architecture and learning method that leverage a very large labeled dataset of faces in order to obtain a face representation that generalizes well to other datasets" (Taigman, Yang, Ranzato, Wolf, 2016, p1). The DNN was trained with 4 million phots of 4.000 Facebook users and reached an accuracy rate of 97,35% which is close to the human accuracy rate. One important improvements to the eigenface it that DeepFace deploys 3-D face models and an mechanism to frontalize the faces on photos where the person does not look straight into the camera (Taigman, Yang, Ranzato, Wolf, 2016). This improvements enables facial recognition in “wild life” and not just under artificial circumstances. Applying Deep Learning algorithm is the state of the art technology for facial recognition technology. Many companies (e.g. Amazon, Microsoft, IBM, Megvii, Facebook and Google) developed facial recognition software with increasingly accuracy rates (Thales, 2020). The market for facial recognition technology is increasing from to 3,8 mrd. $ in 2020 to 8,5 mrd $ in 2025 resulting in a compound annual growth rate of 17,2% (Mehra, 2020).

Facial recognition systems are trained with training data learning which facial feature patterns are most unique. This trained facial recognition system is tested with test data to assure a certain level of accuracy. Finally the trained and tested facial recognition system is deployed and a probe image is compared with a reference dataset to find a match (GOA, 2020). Modern facial recognition technology are matching a saved facial template with a newly captured image of a person and calculating a matching score (similarity between saved facial template and the new image) (Adler & Schuckers, 2007). The facial template is created for every registered identity “by aligning the image and adjusting the color levels to account for different poses or lighting [and] extracting features unique to the face” (GOA, 2020, p. 4). Facial recognition technology can be used for “three types of analytics: verification (matching the ID photo in airports), identification (matching a photo in a database) and classification (gender, age, etc)” (Dushi, 2020, p. 3).

6 Benefits and threats to society using facial recognition technology

Facial recognition technology reduces the time to authenticate a individuum or a group of people significantly with a high accuracy rate (e.g. 97,35% DeepFace) and low costs. The identification is done non-inversive, which means the individuum does not have to touch a fingerprint-sensor or has to show his or her ID-Card. The identification can be proved with any camera making a photo of the individuums face in an acceptable quality. The information about the identity of the people can seamless connected with information about that individuum stored in a database. The combination of identification and the increasingly stored data of each individuum leads to a huge field of applications which may be beneficial for humankind. The biggest benefits for facial recognition technology is the deployment in: authentication security, supporting law enforcement, marketing and retailing and healthcare.

Authentication of persons with facial recognition technology has proven already its market readiness. “Traditional password-based solutions are being predominantly replaced by biometric technology for mobile user authentication” (Rattani, Derakhshani and Ross, 2019, p.1). The progress of camera technology in the last 10 years made it possible to use smartphone cameras for facial recognition authentication. The most popular example is FaceID from Apple . The biometric data is stored locally and is not transmitted to the cloud. The probability that a different person can unlock the phone is 1 to 1.000.000 (Apple, 2020). Other proven use cases for authentication via facial recognition technology are the payment and banking sector. For example payments with Alibaba or transaction via Mastercard can be authorized via facial recognition technology (Kan, 2015 and Lee, 2016). The combination of biometric data (e.g. facial recognition) and a classical password as called multifactor biometrics identification. Multifactor biometrics authentication delivers a high level of security (Itakura and Tsujii, 2005). With facial recognition technology entry control for restricted areas can be easily monitored. A use case for area access control are hotels (Morosan, 2020).

Facial recognition technology is beneficial for securing public safety by supporting law enforcement. Examples for use cases of facial recognition technology in law enforcement are border controls and tracking of suspects or finding missing persons. Facial recognition technology is a powerful tool to find persons. The number of closed circuit television (CCTV) systems increased in the last years significantly in public space. These CCTV Systems can be used to search for persons. In Delhi (India) were a facial recognition system tested using photos of public CCTV systems to track down missing children. In one day the local police found 3000 missing children (Nagaraj, 2020). Facial recognition technology is proven to be efficient to track down suspect of alleged of crimes. 2019 a accused rapist was tracked down in New York within 2 days after the offence was reported (McArthy, 2019). Paris implemented 2009 an automated border control system at the airport in Paris-Charles de Gaulle called PARAF (automated fast track crossing at external borders). This system identifies the incoming passenger from Countries with Visa restrictions via facial recognition technology and cross-checks the identity with the passport of the passengers. The process is fully automated. Therefore no personal is needed and with increasing number of PARAF terminals the waiting time for passengers decrease significantly. Another use case is the identification of citizen when new official documents are issued or for identification of dead persons during a large scale disaster (Khoo, Mahmood, 2020)

In the healthcare sector use cases for facial recognitions technology are the diagnostic for genetic disorders, the monitoring of patients as well as providing useful health indicators to medical experts (Martinez-Martin, 2019). Facial recognition technology can reduce significantly the burden and efficiency to diagnose rare genetic disease. For example the Turner syndrome can be diagnosed with facial recognition technology (Chen & Pan, 2018). A time consuming task for nurses and especially for geriatric nurses is the monitoring of the patient. Has the patient pain, how is the health status, has the patient taken the prescribed medicine? Facial recognition system combined with deep learning algorithm can support the nurses significantly in monitoring the patient. Furthermore health related information like pain or activity of the patient can be assessed and reported. Retirement homes as well as hospitals would benefit from such systems (Hossain, 2015).

For marketing and retailing it is very important to know the customer. Facial recognition technology enables fast identification of persons. Once the identity of a customer is known, information about the needs and the person can be collected to offer the customer what he or she wants. A lot of personal data and preferences are collected of every Facebook user. Combining the identification and the assessing the preferences of customers is a competitive advantage for marketing. Facebook patented such a technology (Dorfer, 2017). The combination of customer identification and the information about the preferences of the customer enables further more a precise target oriented advertisement. For example if a customer walks along a street the monitors close to the customers could displays target oriented advertisement for this specific customer (Reinhold, Herhausen, Pahl, Wulf, 2020). Another interesting use case is the cashier less retail stores. For example Amazon deployed a facial recognition technology in its supermarkets “Amazon Go” tracking the customer and recording which items the customer is buying. If the customer leaves the supermarket the recorded items will be purchased automatically without any cashier (Limer, 2018). Marketing agencies and retail stores would benefit from facial recognition technology while the normal customer could lose potentially her/ his privacy.

Legal concerns and threats for society by applying facial recognition technology “can largely be categorized under the umbrellas of privacy law, human rights issues, and constitutional law” (Chun, 2020, p.109).

Facial recognition has an impact on **privacy** because of data security concerns as well as concerns of the control over personal information. As in chapter 5 explained facial recognition system saves a face template of each registered person. These face template are unique and permanent biometric data of an individuum. If a data breach occurred the biometric identity is revealed and cannot be replaced like a normal password. Therefore a particular focus on data security must be set (GOA, 2020). Another concern is that information about the biometric data or the information generated from a facial recognition system can be “used, shared, or sold in ways that consumers do not understand, anticipate, or consent to” (GOA, 2020, p.14).

Concerns about **constitutional** and **human rights** are manifold: algorithmic bias, mass use for law enforcement beyond the normal scope (mass surveillance, restriction of freedom of movement or freedom of gathering) and discrimination of minorities or oppositions.

The accuracy of the facial recognition system depends on the used deep learning algorithm as well as the amount and quality of the training data (face images). The training data should represent the features of faces for which the recognition system is used for later on. The National Institute of Standards and Technology (NIST) from the USA tested 2019 the accuracy of 189 facial recognition algorithms from 99 developers. The results shows a strong accuracy bias of ethnics. Many algorithms "falsely identified African-American and Asian faces 10 to 100 times more than Caucasian faces" in a one-to-one matches (Wolfe and Dastin, 2019). Especially for darker skinned females are facial recognition system less accurate as for white males (McClellan, 2020). One reason for the ethical inaccuracy of the facial recognition system are the used face images during the training period. In many cases the training data is skewed to white men. Its said that the pioneer of facial recognition technology Mr. Bledsoe used almost entirely white men face images as training data (Raviv, 2020). Having the NIST result in mind, the problem of biased training data and thus inaccurate facial recognition technology still exist. "An [facial recognition] algorithm never returns a definitive result, but only probabilities" (FRA, 2019, p.9). People tend to assume computer based results are mathematically correct and thus highly accurate leading to a reduction of questioning the results (Chun, 2020).

The use of facial recognition technology in law enforcement was debated in the recent years increasingly in Europe and USA. On the one side facial recognition technology can be beneficial for public safety but on the other hand there are fears this technology will be used "far beyond its intended purpose and beyond the scope of protecting the people" (McClellan, 2020, p.375). Therefore a "careful detailed regulation is needed that does not [leave] spaces for misinterpretation" (Dushi, 2020, p.9) in order to enable the law enforcement to protect the citizen the best possible way and addressing the concerns arising with the use of this technology. The European court of human rights developed a three-pronged test which facial recognition system needs to pass to assure that it is not violating human rights: Does the facial recognition system "pursue a legitimate aim; [is it] in accordance with the law, i.e. necessitating an appropriate legal basis meeting qualitative requirements (public, precise, and foreseeable);[is it] necessary in a democratic society (necessity and proportionality test)" (FRA, 2019, p.21). If facial recognition system are deployed which failed the test, serious human and constitutional violation can occur as a result. For example (Dushi, 2020):

- Massive surveillance can breach privacy completely in public space
- Discrimination of minorities or people with facial features detected as being an indices of a criminal
- Causing a feeling of intimidating and intrusiveness limiting the freedom of assembly and movement which is in many countries a constitutional right

In current developments facial recognition technology is connected with other deep learning algorithm to evaluate specific facial or vocal features. For example the facial recognition technology is connected with an algorithm to evaluate the feelings of a restaurant customer to assess the waiter and chefs performance (Chang, Schmelzer, 2019)), or to assess psychological characteristics of an job candidate during an interview (Zetlin, 2018). Furthermore based on the facial recognition technology studies for the pseudoscience physiognomy revived. Physiognomy is a pseudoscience using facial features to “identify character traits, personality traits and temperament, or political and sexual orientation” (Bendel, 2018). This development is seen to be critically for human rights. First the accuracy of these test are questionable (Chinoy, 2019) and second it would open opportunities for mass discrimination in a variety of fields enabling a inhumane system based of suppression and injustice.

7 Existing regulations for facial recognition technology in USA, EU and China

Facial recognition technology is already used in a variety of application. Besides the benefits of this new technology there are concerns and risk on the other hand to be addressed. This chapter describes the existing regulation framework in the three jurisdictions USA, EU und China for facial recognition technology. There are two major critical areas of facial recognition technology which needs to be addressed with sufficient regulation. First how biometric data are processed and second what kind of task the facial recognition system is allowed to fulfill and which tasks should be banned. Most of the existing regulation frameworks targeting the processing of the biometric data like collection, use, storage, scale and security of biometric data.

USA has federal laws and state laws. The federal laws applies to the entire nation and the state laws are laws for each separate states of USA applying to residents and visitors and business entities operating in that state (Diffen, 2020). On the federal level exist currently no laws to regulate facial recognition technology (McClellan, 2020). On the state level exist in some states laws which can be applied to facial recognition. Some state laws “address the collection, use, storage, data sale, and security of the information” (GOA, 2020, p. 41). Other state laws just address issues of notification or consent when facial recognition is used (GOA, 2020). The following Figure 1 summarize the state laws for addressing facial recognition technology.

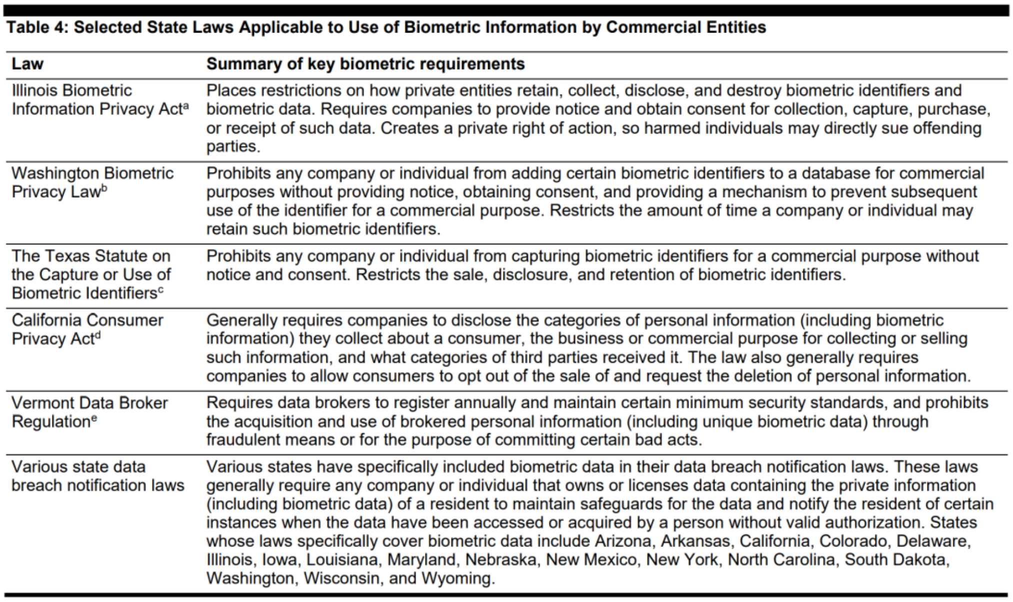

Table 4: Selected State Laws Applicable to Use of Biometric Information by Commercial Entities

Law	Summary of key biometric requirements
Illinois Biometric Information Privacy Act[a]	Places restrictions on how private entities retain, collect, disclose, and destroy biometric identifiers and biometric data. Requires companies to provide notice and obtain consent for collection, capture, purchase, or receipt of such data. Creates a private right of action, so harmed individuals may directly sue offending parties.
Washington Biometric Privacy Law[b]	Prohibits any company or individual from adding certain biometric identifiers to a database for commercial purposes without providing notice, obtaining consent, and providing a mechanism to prevent subsequent use of the identifier for a commercial purpose. Restricts the amount of time a company or individual may retain such biometric identifiers.
The Texas Statute on the Capture or Use of Biometric Identifiers[c]	Prohibits any company or individual from capturing biometric identifiers for a commercial purpose without notice and consent. Restricts the sale, disclosure, and retention of biometric identifiers.
California Consumer Privacy Act[d]	Generally requires companies to disclose the categories of personal information (including biometric information) they collect about a consumer, the business or commercial purpose for collecting or selling such information, and what categories of third parties received it. The law also generally requires companies to allow consumers to opt out of the sale of and request the deletion of personal information.
Vermont Data Broker Regulation[e]	Requires data brokers to register annually and maintain certain minimum security standards, and prohibits the acquisition and use of brokered personal information (including unique biometric data) through fraudulent means or for the purpose of committing certain bad acts.
Various state data breach notification laws	Various states have specifically included biometric data in their data breach notification laws. These laws generally require any company or individual that owns or licenses data containing the private information (including biometric data) of a resident to maintain safeguards for the data and notify the resident of certain instances when the data have been accessed or acquired by a person without valid authorization. States whose laws specifically cover biometric data include Arizona, Arkansas, California, Colorado, Delaware, Illinois, Iowa, Louisiana, Maryland, Nebraska, New Mexico, New York, North Carolina, South Dakota, Washington, Wisconsin, and Wyoming.

Figure 1: State laws addressing facial recognition technology in the USA (source GOA, 2020, p.42)

The California Consumer Privacy Act gives the consumer the right to be informed which data are stored and for which reason the data is collected as well as the right for data deletion. In addition the laws from Illinois, Washington and Texas regulating and restricting the processing of biometric data. The Illinois Biometric Information Privacy Act gives the affected persons the right to directly sue the offending parties. The right for citizen to take action against the offending parties is crucial for an effective protection against criminal use of facial recognition systems.

In the USA as well as in other parts of the world arose discussions about the ban of facial recognition technology. Several cities (e.g. San Francisco, Oakland, Sommerville, Brookline, San Diego) in the USA banned in the last two years facial recognition technology for the use of law enforcement (Schneider, 2020). The European Union (EU) took in consideration to ban facial recognition technology as a whole for 5 years as well. But after reconsideration the EU backs away from the plan to ban facial recognition technology (Espinoza and Murgia, 2020).

The **European Union** passed 2018 the General Data Protection Regulations (GDPR). The GDPR is a “comprehensive data protection and privacy law that applies to all EU member states” (Daigle & Khan, 2020, p. 2). The GDPR assures that privacy is a fundamental right that gives the people the “autonomy, control over private information, and the right to be left alone” (Chun, 2020, p.116). In comparison to the USA state laws (except the Illinois Biometric Privacy Act) the GDPRS assures a strong enforceability leading to over 500 Mio. $ fines till June 2020 (Daigle, Khan, 2020). The GDPR requires consent before personal data is processed. The consent can be withdrawn any time (Gilman, 2018). The data used for facial recognition is classified as biometric data. Processing biometric data is prohibited in article 9. Nevertheless there are 10 exceptions allowing the processing of biometric data, e.g. explicit consent, vital interest, not-for profit bodies, legal claims or judicial acts reasons of substantial public interest, health or social care and public health (GDPR, Art 9). Thus the EU has since 2018 a comprehensive regulation framework to protect biometric data. As mentioned in chapter 6 the European court of human rights developed a three-pronged test for facial recognition technology to assess whether the system violating human rights: Does the facial recognition system “pursue a legitimate aim; [is it] in accordance with the law, i.e. necessitating an appropriate legal basis meeting qualitative requirements (public, precise, and foreseeable); [is it] necessary in a democratic society (necessity and proportionality test)” (FRA, 2019, p.21). This approach can assure that the usage of facial recognition systems are not violating human rights and constitutional rights. The EU is in the beginning of a journey to combine the development of artificial intelligence (AI) (e.g. facial recognition systems) with a well-balanced regulation framework. In February 2020 the EU commission published a white paper for AI and proposed a risk assessment approach for regulation of these new technology. In the next years the regulation framework for AI and facial recognition technology will elaborated and refined (EUC, 2020)

Besides USA and EU is **China** one of the major development areas for AI and facial recognition technology. China’s top legislative body the National People’s Congress (NPC) decided 2012 to protect “electronical data by which the individual identities of citizens can be identified or that involve citizens’ individual privacy” (Zhang, 2013). This decision was transformed into the Cybersecurity law (CSL) which was effective in 2016. The CSL regulates the protection of personal information including biometric data such as facial recognition data. Mainly in article 41 - 45 (chapter IV: network information security) the rules for protecting the personal information are described. The main focus are (Creemers, Triolo, Webster, 2018):

- Storage of personal data unrelated to the provided services is unlawful (Art. 41)
- Personal data can be shared with other companies just with consent of individuum (Art. 42)
- Necessary measurements to secure the personal information and leakage prevention (Art. 42)
- If leakage occur the individuum has to be informed (Art. 42)
- Individuum has the right to demand deletion of personal data when violation occurs or to demand data correction, if saved data is not correct (Art. 43)
- Unlawful acquisition and selling of personal information is banned (Art. 44)

The main focus of this law was the regulation of the use of collected information of network operators (inclusive biometric data which are personal information). The regulation of facial recognition technology is not the central focus of the CSL (Lee, 2020). In recent years the discussions for regulating facial recognition technology and broader artificial intelligence increased. For example 2019 a law professor suit a wildlife park which collected via facial recognition technology the individual characteristics (biometric data) of their visitors compulsory potentially violating consumer protection laws (Allen, 2019). This case lead to a broader discussion about the facial recognition technology in china. This discussion got more intense as more cases of deep fake videos occur violating individual rights. The app Zao for example can swap faces within seconds leading potentially to misuse (Ingram, 2019). The Chinese Government is aware of the need and demand for a centralized data protection law (Lee, 2020). The development plan of the new generations of artificial intelligence stresses that “dual technical and social attributes of AI must be carefully managed to ensure that AI is trustable and reliable” (Wu, Huang & Gong, 2020 p. 303). In March 2020 the state administration of market regulation of the people’s republic of China published the “Personal Information Specifications” a best practice guideline for the protection of personal information including explicit biometric data processed in facial recognition technology. The specification is a guideline for collecting, transmitting, storage and sharing and transferring biometric data. Sheng and Xu summarized the most important points of this guideline:

- “Collection: A personal information controller should separately inform the individual of the purpose, manner and scope of the personal biometric information to be collected and used, as well as storage period and other rules, and should obtain explicit consent from the individual.” (Sheng and Xu, 2020)
- “Storage: Personal biometric information should be stored separately from personal identification information. […].” (Sheng and Xu, 2020)
- “Share and Transfer: As a principle, personal biometric information should not be shared or transferred to any third party. In case it is necessary to do so, the personal information controller will separately inform the individual of the purpose, types of information concerned, identity and capabilities of the third party, and obtain explicit consent.” (Sheng and Xu, 2020)

The Chinese legislative passed the CLS as a basic data protection law and specified best practice guidelines for special issues like facial recognition technology. In comparison to the EU’s GDPR, China does not have “a unified legal framework for data protection driven by a strong emphasis on personal privacy” (Tan, 2020). China did address issues regarding privacy concerns but leaves space for business development at the same time. This discussions are focusing about private companies and not the use of facial recognition technology for law enforcement or other governmental agencies. In fact there are no visible limitation for the use of facial recognition technology for governmental surveillance (Roussi, 2020).

The EU has the most comprehensive regulation framework for privacy rights (GDPR) but is lacking in regulating the applications of facial recognition technology. China discussed in the last years laws for privacy rights in form of data protection laws like the CLS and developed best practice guidelines for facial recognition technology. Nevertheless China lacks completely in regulation for the use of facial recognition technology for governmental use. USA does not have a unified federal law for data protection as well for the regulation of the applications of facial recognition technology. Some state in the USA passed state laws for protecting privacy. The application of facial recognition technology for law enforcement is banned in some cities.

8 A proposal for a regulation framework maximizing the benefits while minimizing or mitigating the risks

Facial recognition technology can be very beneficial for humankind if used within a well-defined regulation framework. Especially in the area of authentication security, supporting law enforcement, marketing and retailing, social media and healthcare facial recognition technology can be applied and assuring the usage of the best state of the art technology serving humankind. On the other hand if the facial recognition technology is used in a manner that privacy rights, human law or constitutional law are being violated this technology has the potential to lead humankind in a dark century with mass surveillance, oppression and discrimination of political opposition and (e.g. ethic) minorities threatening our democracy values. In chapter 7 the existing regulation frameworks in the biggest development centers of AI and facial recognition technology USA, China and EU were discussed. The development of regulation framework for facial recognition technology is in the beginning and not sufficient in any of the three jurisdictions. In the USA and the EU voices promoting banning facial recognition were discussed and e.g. some cities in USA banned the usage of facial recognition technology for law enforcement. Effectively no superordinated ban for facial recognition technology prevailed. A ban is the wrong method to address the issues arising from the usage of facial recognition system. The development of facial recognition technology will not stop if one jurisdiction is banning this technology. Banning this technology would lead to a loss of control over the development of this technology. The most efficient way to reconcile the benefits with the threats is to create a comprehensive regulation framework within this technology can be developed and deployed. Setting standards for a new technology is leading to a big competitional advantage (Kynge & Liu, 2020). The time to set standards in form of a comprehensive regulation framework for facial recognition framework (or more generalized artificial intelligence) is now. Discussion how such a regulation framework can be created are increasingly discussed in the last two years in the three considered jurisdiction USA, China and the EU. One out of 6 main priorities for the European Commission for 2019-24 is digitalization (EUCD, 2019). The European Commission published in February 2020 a white paper about Artificial Intelligence (AI) - facial recognition technology being a part of AI. This whitepaper proposes a regulation frameworks for AI (EUC, 2020). The regulation of AI is being discussed broadly 2020 in the EU (e.g. EUC2, 2020 or Dushi, 2020). In China possible regulatory frameworks for the use of facial recognition technology for private companies (not for governmental use) are discussed intense in the last two years (Wu, Huang, and Gong, 2020). The main focus in China is the implementation of guidelines/ principles driven by Chinas national standard institutions, universities and companies. Chinas ministry of science and technology (MOST) established a expert committee for New Generation AI. This expert committee released principles of next generation AI governance (Bo, 2019; Laskai & Webster, 2019). Universities (e.g. Peking University) and private companies (e.g. Baido, Alibaba, Tencent) developed in the same year (2019) the Beijing AI Principles. This principles focusing on the development, the use and Governance of AI in order for “its healthy development to support the construction of a community of common destiny, and the realization of beneficial AI for mankind and nature” (BAAI, 2019). In the USA the main stakeholder in the are universities, the government (e.g. congress) and private companies. Mrs. Chun (juris doctor candidate North Carolina school of law) proposed a regulation framework worth to be discussed in “Facial Recognition Technology: A Call for the Creation of a Framework

Combining Government Regulation and a Commitment to Corporate Responsibilities" (Chun, 2020). Mrs. Chun proposed a three-pronged regulation framework addressing: government regulation, private companies & developer regulations as well as the sensibilization of end-users/ consumers. Based on a risk assessment of the facial recognition technology the responsibilities for regulation between the government and the private companies/ developers can be distributed. If it is a high risk the regulations behoove the government and if it is a non-high risk the responsibilities for regulation behoove for the companies and developers. Mrs. Chun stresses the importance of "the presence of consumers or users [acting] as drivers of market forces to encourage ethical use and development of facial recognition technology" (Chun, 2020, p. 122). The three pronged-framework addressing the important stakeholder (government, companies and consumer) is a good step towards a comprehensive regulation framework. The explicit regulation from government and the companies as well the inclusion of the consumers in the process is most likely to differ in the three discussed jurisdictions and Mrs. Chun described the explicit regulations more vague. In the following the must component for the regulation of government as well as companies are described in more detail.

Facial recognition technology is leading to concerns about the privacy by processing individual data as well as concerns regarding human and constitutional rights by applying facial recognition technology for example for mass surveillance. The European Union developed a comprehensive law to protect data and thus the privacy (GDPR). The basis of GDPR is the explicit consent. This law is seen as a role model for other jurisdictions like USA (Chun, 2020). To address concerns about the violation of human rights and constitutional rights the risk of the deployment of a specific facial recognition technology has to be assessed as well. Mrs. Chun proposed a governmental regulation based on a risk assessment. The white paper for AI of the EU proposed a "risk-based approach [as well] to help ensure that the regulatory intervention is proportionate" for AI (EUC, 2020, p.16). Nevertheless the EU proposed for facial recognition technology to be always assessed as high-risk and therefore be subject to requirements regarding training data, data & record keeping, information to be provided, robustness & accuracy, human oversight and further specific requirements (EUC, 2020). These requirement should be fulfilled by every facial recognition technology. The potential risk for the misuse of facial recognition technology are significant and therefor it is necessary to apply a basis regulation framework for facial recognition technology. The main components for this regulation could be: transparency through information obligation, robustness and accuracy, human overview, compliance with human and constitutional rights.

The companies has to provide for everyone understandable information regarding the intended purpose, the capabilities and the limitations of the facial recognition technology (transparency through information obligations). People should be informed when they interacting with a facial recognition technology (EUC, 2020). The facial recognition technology must be robust and accurate meaning the system should be fulfill during the full life cycle following requirements: the results has to be reproducible, the level of accuracy should be visible, the system should deal with errors and inconsistencies and should be robust against manipulations (EUC, 2020). The transparency as well as the robustness and accuracy could also be compulsory tested and certified by a third-party test institution (Smith, 2018). For critical cases with a huge effect on affected citizens (like identification in a crime case) human overview has to be compulsory (EUC, 2020). The use of the facial recognition technology has to be within the human as well as the constitutional rights. It has to be forbidden to apply facial recognition technology for discrimination. To assure the compliance with human and constitutional law the European court of human rights developed a three-pronged test for facial recognition technology to assess whether the system violating human or constitutional rights: Does the facial recognition system "pursue a legitimate aim; [is it] in accordance with the law, i.e. necessitating an appropriate legal basis meeting qualitative requirements (public, precise, and foreseeable); [is it] necessary in a democratic society (necessity and proportionality test)[?]" (FRA, 2019, p.21). The basic rules protects the citizens and legal entities against the violation of there rights and democratic freedoms and supporting an environment where developed facial recognition technology can be accepted and trusted.

The companies and developer has to be compliant with the regulation framework set by the government. In addition companies and developer should follow standards for developing, distribution and using facial recognition technology. Following well defined standards is a competitional advantage since the customer can rely on predefined quality and ethical standards. The introduction of the quality norm ISO 9000 can be an explanatory example. As described in chapter 7 a broad discussion arose in China about standardizing AI like the Beijing AI Principles (BAAI, 2019). The European commission introduced ethical guidelines for trustworthy AI in 2019 (EUC2, 2019). In the USA the discussion is lead by the big technology companies such as Windows calling for a regulation framework as well as introducing principles for the responsible development and use of facial recognition technology (Smith, 2019). The standardization process for facial recognition technology is in a early stage and will develop in the near future. It is most likely that different standards will coexist and compete with each other. To assure the success of comprehensive and meaningful standards all stakeholders (government, companies and developer, as well as the users) should participate in the discussion. The user or consumer "could act as drivers of market forces to encourage ethical use and development of facial recognition technology" (Chun, 2020, p. 122). Therefore the user should be enabled to understand and assess facial recognition technology. A crucial role in providing information about the technology and the standardization process are consumer advice centrals. Furthermore consumer advice centrals could fight for the rights of the end user of facial recognition technology. The end user should easily be able to access whether the facial recognition technology are in compliance with their interests. Labeling of facial recognition technology by consumer advice centrals would enable a fast assessment of the specific technology (EUC, 2020). Furthermore citizens should learn more about facial recognition technology in order to assess and be aware of potential risks. A possibility is to teach basics of artificial technology such as facial recognition technology in high school.

9 Conclusion

The research essay proposed a regulation framework for facial recognition technology to maximize the benefits of this new technology while minimizing or mitigating the risks. The main benefits of facial recognition technology arise with their applications. Facial recognition technology is very beneficial for authentication security, supporting law enforcement, marketing and retailing, social media and healthcare. On the other hand facial recognition technology could lead to tremendous threats to democratic societies by endangering privacy rights of citizens and violating human as well as constitutional laws. In a worst case scenario facial recognition technology can lead to mass surveillance, discrimination of (e.g. ethical) minorities and oppression of opposition and democratic rights. Banning facial recognition to counter the threats is illusory since the development of this technology will not stop. The best way to maximize the benefits of the facial recognition technology while minimizing or mitigating the risk is to create a comprehensive regulation framework in which the technology can be developed and serve humankind the best possible way. The research proposed a three-pronged (compare Chun, 2020) approach: Governmental laws, standards for companies and developer and the purchase power of aware and informed customers. The government should create a basis framework of regulation including: transparency through information obligation, robustness and accuracy, human overview, compliance with human and constitutional rights. Since now neither in the USA, EU or in China are comprehensive laws addressing this issues are passed. The concrete formulation of this laws should be discussed and passed within in the next years. The companies and developer should follow standards and should be certified. Different standards are already created. In the next years the suitability of those standard should be tested and the best standards should prevail. The consumer has a crucial role monitoring both governmental legislation as well as corporate behaviors. In order to enable the consumer to be a competent stakeholder in the process basic understanding of artificial intelligence such as facial recognition technology should be taught in high school. Consumer advice centers should be empowered to provide comprehensive information's to customer and to fight juridically on behalf of consumers against companies or governmental regulation.

10 Library

- Adler, A., Schuckers, S., Comparing Human and Automatic Face Recognition Performance, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS, VOL. 37, NO. 5, OCTOBER 2007
- Allen, K., (2019), China facial recognition: Law professor sues wildlife park, https://www.bbc.com/news/world-asia-china-50324342 (last access: 08.11.2019)
- Apple (2020), Informationen zur fortschrittlichen Technologie von Face ID , https://support.apple.com/de-de/HT208108 (Last access: 16.12.2020)
- BAAI – Beijing AI Principles (2019), Bejing AI Principles, https://www.baai.ac.cn/news/beijing-ai-principles-en.html (last access: 19.12.2020)
- Bala, N., 2020, THE DANGER OF FACIAL RECOGNITION IN OUR CHILDREN'S CLASSROOMS, Duke Law & Technology Review
- Bendel O. (2018), The Uncanny Return of Physiognomy, AAAI Spring Symposium Series
- Bo, Xiang (2019), China issues principles of next generation AI governance, http://www.xinhuanet.com/english/2019-06/18/c_138152819.htm (access: 19.12.2020)
- Böckler, S. (2020), DERMALOG provides the worlds first biometric border control system with integrated fever detection, https://www.dermalog.com/news/article/dermalog-provides-the-worlds-first-biometric-border-control-system-with-integrated-fever-detection (last access: 21.12.2020)
- Chang, W., Schmelzer, M., Kopp, F., Hsu, C., Su, J., Chen, L., Chen, M. (2019), A deep learning facial expression recognition based Scoring System for Restaurants, ICAIIC
- Chen, S., Pan, Zx., Zhu, Hj. et al. Development of a computer-aided tool for the pattern recognition of facial features in diagnosing Turner syndrome: comparison of diagnostic accuracy with clinical workers. Sci Rep 8, 9317 (2018). https://doi.org/10.1038/s41598-018-27586-9
- Chinoy, Sahil, 2019, The Racist history behind facial recognition, https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html (last access: 17.12.2020)
- Chun, S., (2020), Facial Recognition Technology: A call for the creation of a framework combining government regulation and a commitment to corporate responsibilities, North Carolina Journal of Law & Technology
- Creemers, R., Triolo, P., webster, G., 2018, Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (last access: 18.12.2020)
- Daigle, B. Khan, M., 2020, The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities
- Diffen, 2020, https://www.diffen.com/difference/Federal_Law_vs_State_Law#:~:text=Federal%20law%20is%20the%20body,with%2C%20United%20States%20federal%20law. (last access 17.12.2020)

- Dorfer, S., 2017, Facial Recognition Tech : 2018 Could be Crunch Year, https://www.stylus.com/ttybfh (last access: 16.12.2020)
- Dushi, D. (2020), The use of facial recognition technology in EU law enforcement: Fundamental rights implications, Global Campus – South East Europe
- Espinoza, J., Murgia, M., 2020, EU backs away from call for blanket ban on facial recognition tech, https://www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5 (last access: 17.12.2020)
- EUC- European Commission, 2020, White Paper – On Arificial Intelligence – A European approach to excellence and trust
- EUC2- European Commission (2020), Ethics Guidelines for trustworthy AI, https://knowledge4policy.ec.europa.eu/publication/ethics-guidelines-trustworthy-ai_en (last access: 19.12.2020)
- EUCD European Commission (2019), A Europe fit for the digital age https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en
- FRA- European Union Agency for fundamental rights, 2019, Facial recognition technology: fundamental rights considerations in the context of law enforcement, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf (last access: 17.12.2020)
- GDPR, 2018, https://gdpr-info.eu/art-9-gdpr/ (last access: 17.12.2020)
- Gilman, M., 2018, Five Privacy Principles (from the GDPR) the United States Should Adopt to Advance Economic Justice
- GOA- United states Government Accountability Office, 2020, Facial Recognition Technology: Privacy and Accuracy Issues related to commercial uses, Report to Congressional Requesters
- Goldstein, A., Harmon, L., Lesk, A., (1971), Identification of Human Faces
- Hossain, M.S., Muhammad, G. Cloud-Assisted Speech and Face Recognition Framework for Health Monitoring. Mobile Netw Appl 20, 391–399 (2015). https://doi-org.pxz.iubh.de:8443/10.1007/s11036-015-0586-3
- Ingram, D. (2019), A face-swapping app takes off in China, making AI-powered deepfakes for everyone, https://www.nbcnews.com/tech/security/face-swapping-app-takes-china-making-ai-powered-deepfakes-everyone-n1049501 (last access: 18.12.2020)
- Itakura, Y., Tsujii, S. (2005), Proposal on a multifactor biometric authentication method based on cryptosystem keys containing biometric signatures,
- Kan, M. (2015), Alibaba uses facial recognition tech for online payments, https://www.computerworld.com/article/2897117/alibaba-uses-facial-recognition-tech-for-online-payments.html (Last access: 16.12.2020)
- Khoo, L., Mahmood, M. (2020), Application of facial recognition technology on identification of dead during large scale disasters, Forensic Science International
- Kynge, J., Liu, N. (2020), From AI to facial recognition: how China is setting the rules in new tech, https://www.ft.com/content/188d86df-6e82-47eb-a134-2e1e45c777b6 (last access: 19.12.2020)

- Laskai, L, Webster, G (2019), Translation: Chinese Expert Group Offers 'Governance Principles' for 'Responsible AI', https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-expert-group-offers-governance-principles-responsible-ai/ (last access: 19.12.2020)
- Lee, J. (2016), Mastercard introduces facial recognition mobile payments in Europe, https://www.biometricupdate.com/201610/mastercard-introduces-facial-recognition-mobile-payments-in-europe (Last access: 16.12.2020)
- Lee, S. (2020), Coming into Focus: China's Facial Recognition Regulations, https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations (last access: 18.12.2020)
- Limer, E., 2018, Amazon's Smart Convenience Store Has Some Scary Implications, https://www.popularmechanics.com/technology/design/a15840204/amazon-opens-amazon-go-seattle/ (last access: 16.12.2020)
- Martinez-Martin, N. (2019), What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?, AMA J Ethics
- McCarthy, C. (2019), "Facial recognition leads cops to alleged rapist in under 24 hours", https://nypost.com/2019/08/05/facial-recognition-leads-cops-to-alleged-rapist-in-under-24-hours/ (last access: 15.12.2020)
- McClellan, E. (2020), Facial Recognition Technology: Balancing the Benefits and Concerns, Journal of Business & Technology Law
- Mehra, A (2020), Facial Recognition Market, https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp (last access: 15.12.2020)
- Morosan, C. (2020), Hotel facial recognition systems: Insights into guests' system perceptions, congruity with self-image, and anticipated emotions, University of Houston
- Nagaraj, A. (2020), Indian police use facial recognition app to reunite families with lost children, https://de.reuters.com/article/us-india-crime-children/indian-police-use-facial-recognition-app-to-reunite-families-with-lost-children-idUSKBN2081CU (last access 15.12.2020)
- Ramco, (2020), Discover RamcoGEEK – Comprehensive Pandemic Control System, https://ramco.com/hcm/pandemic-control-system-for-workplace-safety-and-employee-health/ (last access: 21.12.2020)
- Rattani, A. Derakhshani, R., Ross, A. (2019), Chapter 1 - Introduction to Selfie Biometrics, , https://doi.org/10.1007/978-3-030-26972-2_1
- Raviv, S. (2020), "Secret History of Facial Recognition", https://www.wired.com/story/secret-history-facial-recognition/ (last access: 15:12.2020)
- Reevell, P. (2020), How Russia is using facial recognition technology to police its coronavirus lockdown, https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736 (last access: 21.12.2020)
- Reinhald, M., Herhausen, D., Pahl, M, Wulf, J., 2020, Perspektiven für Face-Recognition im Data-Driven-Marketing, Marketing review St. Gallen

- Roussi, A. (2020); Resisting the rise of facial recognition, https://www.nature.com/articles/d41586-020-03188-2 (last access: 18.12.2020)
- Schneider, B., 2020, We're Banning Facial Recognition.We're Missingthe Point., https://www2.cs.duke.edu/courses/spring20/compsci342/netid/news/nytimes-schneier-facial.pdf (last access: 17.12.2020)
- Schumacher, J. (2020), Übermittlung von Corona-Daten: Anschluss nur per Faxgerät, https://www.ndr.de/nachrichten/schleswig-holstein/Uebermittlung-von-Corona-Daten-Anschluss-nur-per-Faxgeraet,gesundheitsaemter112.html (last access: 21.12.2020)
- Sheng, J., Xu, C. (2020), China Publishes Best Practices for Protection of Personal Information, https://www.pillsburylaw.com/en/news-and-insights/china-publishes-best-practices-for-protection-of-personal-information.html (last access: 18.12.2020)
- Smith, B. (2018), Facial recognition: It's time for action, https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/ (last access: 20.12.2020)
- Taigman, Y., Yang, M., Ranzato, M., Wolf, L (2016), DeepFace: Closing the Gap to Human-Level Performance in Face Verification
- Tan, M., (2020), China: facial recognition and its legal challenges, https://www.taylorwessing.com/de/insights-and-events/insights/2020/05/china---facial-recognition-and-its-legal-challenges (last access: 18.12.2020)
- Thales (2020), PARAFE: a new generation of smart gates for the ADP Group, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/smart-gates-paris (last access: 16.12.2020)
- Thales, (2020), Facial recognition: top 7 trends (tech, vendors, markets, use cases and latest news), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition (last access 15.12.2020)
- Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., Struble, M., Vanam, V., Vattikonda, N., (2020), The rise and regulation of thermal facial recognition technology during the COVID 19 pandemic, Journal of Law and the Biosciences 1-17, doi:10.1093/jlb/lsaa038
- Wolfe, J., Dastin, J. (2019), U.S. government study finds racial bias in facial recognition tools, https://www.reuters.com/article/us-usa-crime-face-idUSKBN1YN2V1 (last access: 16.12.2020)
- Wu, W., Huang, T., Gong, K. (2020); Ethical Principles and Governance Technology Development of AI in China, Chinese Academy of Engineering and Higher Education Press Limited
- Zetlin, M., 2018, AI is now analyzing candidates' facial expression during video job interview, https://www.inc.com/minda-zetlin/ai-is-now-analyzing-candidates-facial-expressions-during-video-job-interviews.html (last access: 17.12.2020)
- Zhang, L., 2013, China: NPC Decision on Network Information Protection, https://www.loc.gov/law/foreign-news/article/china-npc-decision-on-network-information-protection/ (last access: 18.12.2020)