Facial Recognition in Educational Context

The Complicated Relationship Between Facial Recognition Technology and Schools

Shuran Zhao[1]

[1] *Digital Humanities, King's College London*
Email: shuran.zhao@kcl.ac.uk / k19009936@kcl.ac.uk

ABSTRACT

Facial recognition (FR) technology has been available in public for years. People hold differing attitudes towards the use of FR technology, as it has the potential to assist society as well as poses ethical threats. By analysing two recent cases of FR technology in campus, this study examines the complex relationship between FR technology and education. Although the deployment of FR in campus has been criticized due to the technical biases and ethical concerns, there are certain apparent 'good-fits' between them, and to a large extent, this particular context can provide a form of "infrastructural ease" for introducing the FR technology.

Keywords: *Facial recognition (FR), Education, Relationship, Technical bias, Ethical concerns, Infrastructural ease*

1. INTRODUCTION

Facial Recognition (FR), as a novel but increasingly contentious biometric technique, can recognize human face via digital photos and video frames, thus probably leading to constant digital surveillance and an invasion of personal privacy. Over the last decade, it has been widely used in police enforcement, border control and security, business, education and etc. In educational context, obviously, the relationship between schools and FR technology is complicated: on the one hand, there are several obvious "good-fits" between them; but on the other hand, this will inevitably harm the school's 'pure environment'. This study will examine two significant cases of FR technology in schools: (1) the Smart Eye system in Hangzhou Number 11 High School and (2) the AEGIS system deployed in a New York School District, to explore the relationship between FR technology and education. It will first introduce FR technology, then present its background information as well as ethical considerations raised by the two cases. Finally, it will summarize the findings and proposal several suggestions to high-tech corporations, governments, and the general public. Through a socio-technical view, this study critically examines the use of facial recognition technology in education, which aims to improve public deep understandings of AIED (AI in education) and present recommendations for the industry.

2. BACKGROUND: FACIAL RECOGNITION TECHNOLOGY

Over the past decade, FR technical devices has been widely applied in various uses in public. For instance, FR technology used in Australian coffee shops is to detect regular customers (without their knowledge) and provide a personalized retail experience [1]. In China, the Alipay app provides pay-by-face technology, but particularly shoppers are reluctant to use its FR machines and wondering how to turn it off on Weibo [2]. U.S. police departments now use facial recognition cameras to find prospective criminals and locate missing people [3]. As can be seen from these examples, with worldwide usage of FR technology, new FR applications are emerging as well.

2.1. How Does FR Technology Work?

In a nutshell, facial recognition works by computationally extracting facial attributes from a digital image or video frame, and comparing these unique 'face-prints' with features previously stored in a database to analyze facial images [4]. To be more specific, FR technology usually contains four steps: (1) face detection, (2) face alignment, (3) feature extraction, and (4) feature matching [5].

FR systems must first understand what a face is and how to locate it in digital images. To achieve this, designers of facial recognition systems train an algorithm based on millions of recognized human face images [6], using profile photos and selfies of individuals who are frequently active on online platforms. With sets like Facebook, Google, Flickr, Instagram and etc., billions of face images that possessed by the Internet have been integrated into huge images databases [6], but these data used as raw materials to train and improve algorithms can that recognize our own faces without our knowledge.

When it comes to face alignment, the system compares the results with the collected data, once the face in the image has been identified, the system continues to monitor it to choose the optimal angle and visual quality [7]. Here, the FR technique focuses on each person's face. The algorithm is trained to assess whether a photograph is of the same person, despite any ‘noise' existing in the image, such as poor lighting, covered or unnatural expressions [7]. Over many rounds of training, FR systems are fed a range of facial images and know how to distinguish between them [6].

In the feature extraction stage, the facial recognition system identifies the geometric structure of human faces with specific features, such as the nose shape or the width between the nose, eyes, mouth and chin [8]. These identifiable and distinct characteristics can be utilized to distinguish among people.

In the final step, each individual "face-print" is compared to images in the database. The software then determines if this sample corresponds to any specific individual stored in the data archive.

2.2. The Background of FR in Education

Indeed, many high-tech companies have successfully applied their products to the educational seetings: Suspect Technologies, Face-Six, FaceFirst, and other consumer enterprises are concerned about the education market from nurseries, high schools to univeristies. This may not come as a surprise, as FR-based digital surveillance is becoming increasingly commonplace for student safety protection [4]. However, in addition to campus security, FR technology is also being utilized for attendance checking and smart classrooms construction.

As previously stated, one of the most common applications of FR in the education is campus security. This type of technology is frequently implemented in the United States, where public concern over school shootings has prompted its widespread adoption. The school security sector spends $2.7 billion each year [9], and according to the Pew Research Center, 57 percent of teens are concerned about the likelihood of a school shooting [10]. As a result, facial recognition systems are being deployed to control access to campuses (such as SARF and Face-Six), identify unauthorized invaders (like AEGIS and FaceFirst system), and trace students' on-and-off campus activities (such as SARF and Gaggle). The employment of FR technology to schools is supposed to be a solution for preventing school shootings and ensuring campus security. It is expected that safe, accurate FR systems will improve school safety, as promised in some of the marketing campaigns for FR products [11].

Attendance monitoring is another implementation of FR technology in schools. Since monitoring the attendance of a large number of students is a time-consuming work, FR technology is being used as a solution to the manual recording challenge [12], such as the inevitable gaps and omissions in man-made statistics [4]. This type of FR technology application is most prevalent in Western Europe, Asia and Australia, in which with relatively few school shootings and invasions. Spanish tech company Kimaldi, for instance, has developed its FaceGo terminal, a facial biometric technology, to help schools count teachers and students who are absent or late [13]. The FR system ‘LoopLearn' is being tested in 100 schools across Australia and the company behind ‘LoopLearn' claims that its product will save teachers 2.5 hours each week [5]. The University Utara Malaysia also plans to deploy FR technology to monitor its students’ attendance for reducing fraudulent attendance (where a student skips a class and then asks help from a friend who is in class to sign the attendance sheet). Nurul Husna Mohd Fauzi, a final year student in the university and designer of this smart system, states that it will not only help to obviate fake attendance but greatly reduce paper waste, thereby helping to protect our planet [14].

The final application of FR technology in education aims to improve smart classrooms, so that providing a ‘personalised pedagogical support' through automatic facial detection [15], and a growing number of scholars and designers are taking an interest in this area. Dewan et al. [15] have reviewed facial detection algorithms in an online learning context. Learners' brief facial motions are captured by face recognition cameras, which are then matched to a database. The faces will then be classified into various states, boredom, frustration, delight, neutrality, or confusion, which can be employed as an indicator of the learner's participation in the virtual learning environment [15]. In addition to online schooling, FR technology has also been deployed in the real-life learning context. For example, students’ attentiveness monitor known as ‘Smart Classroom Behavior Management System’ or ‘Smart Eye’, is in use at No. 11 Middle School in Hangzhou, China [16]. This system is supposed to become a teacher's assistant, supporting classroom tasks. From above analysis, face recognition is used in three key areas of educational context: campus security, attendance monitoring, and smart classrooms construction. The following part will conduct case analysis of two recently implemented FR systems to reveal the complex relationship between FR technology and the school context.

3. EXAMPLE A: AEGIS FACIAL RECOGNITION SYSTEM IN THE LOCKPORT CITY SCHOOL DISTRICT

Due to frequent shootings at schools, the Lockport City School District (LCSD) in western New York decided to install an AEGIS FR security system starting in March 2018. SN Technologies, a technology firm based in Canada, provided this system. The system itself roughly cost Lockport $1.4 million, funded by the New York Smart Schools Bond Act, an act used to help state schools improve their instructional technology [17].

In terms of this system, director Michelle Bradley said that it was intended to keep those destructive people outside the district [18]. By deploying the AEGIS security system, the district identified unauthorised intruders and protected campus safety. The system would be applied in eight schools in the district, throughout the buildings rather than in classrooms [19].

This is not a facial recognition camera; instead, an algorithmic software integrated into current school CCTV systems [18]. It is designed to recognize the faces of those forbidden from Lockport schools and alert officials when they are spotted on campus, such as sexual offenders, suspended students and employees, and anyone else deemed a threat [19]. Moreover, the technology can also detect firearms.

When the system detects faces that match those on the watchlist or discovers guns, it will automatically initiate a two-step threat confirmation process: first, it alerts human monitors, who confirm or deny the threat; second, if the program detects a weapon, it will alert monitors as well as law enforcement; and district administrators will instantly lock down the campus [18]. Lockport City School District planned to pilot AEGIS in schools on June 3 2018, with the goal of implementing it by September 1st, before the start of the new school year [20].

Since LCSD unveiled its plans in 2018, the accuracy of AEGIS was locked into a bitter dispute. A Lockport neighbor, whose younger daughter was a sophomore at the local high school, spoke to CNN about the software, describing it as ‘a stupid waste of money’ and ‘Big Brother in real life’ [20]. Apart from parents, the system had also been debated by professionals and human rights groups. The New York Civil Liberties Union (NYCLU), fretted about the technology would reinforce racial profiling and biases [20], and the legal counsel of the NYCLU told CNN that FR technology, even the most advanced systems, had been proved to be inaccurate when it came to identifying women and people of colour [20].

The LCSD eventually started classes in September without the controversial deployment of AEGIS technology. The State Education Department mandated the LCSD to stop testing and using FR technology until further notice [21]. The NYCLU requested the Lockport district and The State Education Department for more information, but the response of LCSD left more questions than answers: 'some of the information even included passwords that we weren't supposed to see', a staff member said [20]. As a result, the AEGIS security system tends to be a non-transparent ‘black box’, as both the firm and the district are preserving secrets.

4. EXAMPLE B: SMART CLASSROOM BEHAVIOUR MANAGEMENT SYSTEM

Since the end of March 2018, Hangzhou Number 11 High School in eastern China had installed a FR system in the classroom to monitor students' attentiveness. It's known as the 'Smart Classroom Behavior Management System,' or simply 'Smart Eye'. Three cameras are deployed above the blackboards in the classroom to scan students' faces every thirty seconds, analyzing their facial expressions to detect their emotions [22]. During each lesson, the device may detect seven different emotions and then record them, including Neutral, pleased, sad, disappointed, angry, afraid, and shocked [16]. If the system detects a student being distracted in class, the teacher will be notified and able to intervene (for example, reminding students to improve concentration) [16].

Unlike the western world, Chinese classrooms tend to have numerous students due to country’s large population [23]. Indeed, the average high school class size across Chinese 27 provinces topped 45 students in 2017 [23], whereas the average secondary school class size in England was 21.2 in 2018 [24]. As a result, Chinese teachers in these "super-sized" classes find it difficult to keep a close eye on each student. The school in Hangzhou expects that its FR system will aid teachers in supervising student performance in class.

The increased monitor of the Smart Eye system has greatly changed students’ behaviours. One student explained: ‘Previously, when I had classes that I didn't enjoy, I would be lazy and maybe take naps on the desk, or browse other textbooks. But, since the cameras were implemented in the classrooms, I daren’t to be distracted. It's like a pair of mysterious eyes have been watching on me [16]. This raises another question: do people act differently when they are being observed? The answer is, to a considerable part, yes. So, will students become performers when they are monitored by the Smart Eye system? Will they behave differently than what they used to do? These are issues that the school management team must address.

There is no doubt that the school’s action of employing the system has sparked controversy on social networking sites, with Chinese netizens expresing their fears about constant surveillance and invasion of their privacy. On Sina Weibo, one user wrote that this was more terrifying than being in jail [22]. The good news is that the Chinese government has responded to objections about the use of FR devices in schools by announcing measures to restrict and regulate FR technology and other similar applications [25]. Mr. Lei, director of the Science and Technology Department of Chinese Ministry of Education, also advised schools to be more cautious while using high-tech software [26].

FR is used for different purposes in the United States and China, but both their implementations have caused public fears. Despite the fact that both governments are attempting to play a more active role in technology regulation, public concerns continue to increase. The ethics of FR may be the most pressing concern for citizens.

5. ETHICAL ISSUES

Ethical problems raised by FR are causing increasing controversy in academia, especially with the growing deployment of FR in a variety of social settings. Advocates of FR technology claim that it can dispel human biases from decision-making process [27], but the technology is not always as simple and neutral as it appears. In this regard, this section will examine the ethics of FR technology from two perspectives: first, the technical bias, and second, the social and ethical concerns associated with the two key FR technology application cases described above.

5.1. Technical Bias: Racial and Gender biased Algorithms

Facial Recognition is not a purely technical application as human efforts are involved in the whole process. Indeed, from the very beginning, FR technology learns ‘what a face is’ from the data selected by human beings. According to Boulamwini, machine learning algorithms focus more on statistically over-represented groups: if the male population is heavily overweighted in the training dataset, the system will give greater attention towards statistical relationships for males rather than females [28]. Another research finds that even some of the most advanced facial recognition software tends to have a 35% error rate in identifying dark-skinned women, compared to a 1% error rate for white men [29]. These findings reveal that ‘selection bias’ does exist in most FR systems, as they frequently ‘prefer’ white men and are more likely to misidentify dark-skinned women.

A majority of researchers have strengthened their concerns about this bias, which they believe is extremely perilous. If certain types of faces, such as Black, Asian, ethnic minority or feminine faces, are under-represented in Live Facial Recognition (LFR) training datasets, then this bias will affect the use of the technology [30]. These concerns are not unfounded. Idemia's FR software, which serves the police in France, Australia, and the United States, has been found the difficulty in recognizing black faces equally [31], while the FR system implemented by the Metropolitan police in east London has also been found to misidentify certain groups of people [32]. Therefore, biased algorithms can lead to unequal and unfair treatments for differential social and ethnic groups [33]. If we deploy FR technology in schools, our children may be subjected to racial and sexual discrimination at an early age.

5.2. Technical Bias: Value-laden System

Since designers label various training data through deep learning processes, human biases and cultural assumptions are conveyed in classification choices [33]. Thus, FR systems are value-laden, with their design and functionality reflecting the value and attitudes of designers [34]. Moreover, the subset of the population that design FR algorithms is very limited. The Artificial Intelligence (AI) industry is a male-dominated field, most AI developers are male with high salaries and similar technical and academic background, regardless a paucity of women and minorities in this field [33]. The needs, interests, life experiences, values, and even prejudices of this group are inevitably reflected in the AI which they create.

There is a form of social constructivism that views ‘human action as being mutually shaped by technology’ (p.760) [35]. We've been aware that designers shape the algorithm FR, but will this biased system shape its target audience? Will students' behavior and thoughts be affected by exposure to this technology over time? We need to consider these questions before implementing FR technology into the campus.

5.3. Social and Ethical Concerns: Constant Digital Surveillance

Today's schools are being furtively infiltrated by the monitor system [36], especially with the deployment of FR cameras and algorithms, where students are increasingly surveilled. A variety of technologies are being used in educational contexts to monitor students’ behaviours, as well as understand their thoughts. Surveillance is now ubiquitous. Despite the fact that most technologies are utilized nominally to improve the quality of the school experience, fears of constant digital surveillance are increasing. Indeed, as Chinese Internet users concern, schools are becoming places of detection rather than learning [37]. We can say that these systems are a form of superpanopticon, ‘a system of surveillance without walls, windows, towers or guards’ (p.93) [38], which gives too much pressure on students and produces a tense atmosphere in campus.

Some educators have pointed that algorithmic FR technology is unacceptable in campus [4], which reflects the ambition to control and standardise students' actions.

This concern is reasonable as in the Smart Eye system, for example, stydents' only choice during class is attentiveness. If they have other thoughts, the Smart Eye technology will detect this and send an alert to the teachers. Apart from direct control, these LFR systems may also elicit a sense of self-control in users. In Foucault's 'disciplinary modern society', 'self-control' is also a flexible control technique [39]. As opponents of LFR in schools concern, the usage of algorithmic control techniques will make schools become more terrifying than jails.

5.4. Social and Ethical concerns: Privacy Invasion

Another public concern regarding the application of FR technology is its invasion of privacy. In fact, FR technology operates on the basis of data mining, after scanning human faces, the software is able to recognise, store and track human's biological and behavioural traits that distinguish people from others [30]. As biometric data is stored in public databases available to certain companies, agencies and governments, individuals are losing the control of their former private data. In this regards, individual data privacy and data mining, to a large extent, is a collision process [40], but part of the reason which data mining works is that users unconsciously 'agree' to give up some of their privacy. This unilateral compromise, even blatant invasion of privacy, has raised public concerns.

Returning to the specific context of the school, the majority of FR users are juveniles, and many parents are anxious about the potential misuse or reuse of collected data and its sequent consequences [41], especially for commercial purpose. Although there has not yet been any scandal of misuse and reuse of students' data, the public has already strengthened concerns about the security of such a 'biometric-based identifier' (p.335) [41]. This may be caused by the lack transparency of the AI system. To be more specific, we have no idea what happens to our data after it is collected, where it will be stored, or how long it will be kept. Students, parents and other users are unaware of the information before or even after they are scanned by the system.

5.5. The 'Good fit' Between Facial Recognition Technology and Schools

Despite the ethical issues outlined above, the school, to some degree, is a conducive context for the introduction of FR technology. Schools have a long tradition of monitoring their students and today's students is also likewise accustomed to being watched. CCTV cameras and other monitor systems have indeed long been used in schools, and the images of students' faces have been regularly collected and stored [4]. Facial images, names, and other identifying information are matched and stored on students' school ID cards, access cards, and other systems. Existing name-and-face photographic databases make it easier for FR to be embedded in. Moreover, schools are public spaces with relatively stable populations. As a result, compared to open voids like hospitals or stadiums, FR technology can be more readily employed in these 'stable' institutions [4]. Therefore, schools to a large extent offer some 'infrastructural ease' for implementing FR technology.

6. REGULATION

Given public concerns over the application of FR in schools, governments, social institutions, and experts are collaborating to construct regulations for the industry. In the United States, a leading country in AI field, some state governments have taken steps to limit the use of FR. The New York State Senate enacted a bill (A6787B) on June 20 2019, to ban the use of FR technologies in primary and secondary schools [42]:

Public and nonpublic elementary and secondary schools, including charter schools, shall be prohibited from purchasing and utilizing biometric identifying technology for any purpose, including school security, until July 1, 2022.

More than that, a commission is established to inspect whether biometric technology is appropriate in New York schools, and if so, what rules should be formulated to restrict its usage [43]. This proposed regulation will contribute to protecting teenagers' privacy and allaying public concerns about the usage of FR in campus.

Unlike the US, China currently has no specific laws governing the use of FR technology in education. This means that private companies and schools can continue to use it without notifying the authorities. Despite the fact that China has proposed the 'Beijing AI Principles' as an initiative for Chinese AI industries, 'calling for its healthy development to support the construction of a human community with a shared future, and the realization of beneficial AI for humankind and nature' [44], there is no legislation to limit the applications of FR in the specific educational context.

7. CONCLUSION

FR technology has been deployed in education for a long period of time, despite some disputable applications of FR in campus, several cases prove that it has been operating consistently. This study finds that: (1) the public has an ambivalent attitude towards the deployment of LFR in campus: on one hand, the public expects FR to be a solution to school shootings or other security problems; on the other hand, they fear and distrust facial recognition in schools; (2) there are less conversations among schools, students, parents, related experts and the high-tech firms providing the FR technology before the systems are tested and used; lack of transparency, that is, these tech companies rarely tell their target customers about the systems and shield their technology from public scrutiny (3) although FR has been criticized due to its technological bias and ethical problems, the school's unique context can provide a kind of 'infrastructural ease' for the introduction of FR technology.

For high-tech firms or suppliers, this study recommends that they should subject their systems to public scrutiny and negotiate contracts with users before their FR system is implemented. The general public, particularly students and parents who will be scanned by the FR technology employed in campus, should be aware of what will happen with their data, how their biometric data will be collected, where will it be stored and what are the risks of being scanned. For governments, they should legislate for the application of FR technology and require agencies to conduct an impact assessment before deploying it. Lastly, for the public, we should treat FR technology objectively and rationally, without excessive bias and fears.

REFERENCES

[1] Devlin, P., 2017. The new face of coffee: Sydney Cafe uses facial recognition technology to remember your favourite drink after staff kept forgetting customers' names. [online] Available at: https://www.dailymail.co.uk/news/article-4860082/Sydney-face-using-facial-recognition-coffee.html [Accessed 2 January 2020].

[2] Xie, Y.F., 2020. In China, Paying With Your Face Is Hard Sell. [online] Available at: https://www.wsj.com/articles/in-china-paying-with-your-face-is-hard-sell-11600597240 [Accessed 2 June 2021].

[3] Collins, T., 2019. Facial recognition: Do you really control how your face is being used? [online] Available at: https://eu.usatoday.com/story/tech/2019/11/19/police-technology-and-surveillance-politics-of-facial-recognition/4203720002/ [Accessed 4 January 2020].

[4] Andrejevic, M. and Selwyn, N., 2019. Facial recognition technology in schools: critical questions and concerns, Learning. Media and Technology, DOI: 10.1080/17439884.2020.1686014.

[5] Brownlee, J., 2019. Gentle Introduction to Deep Learning for Face Recognition. [online] Available at: https://machinelearningmastery.com/introduction-to-deep-learning-for-face-recognition/ [Accessed 2 January 2020].

[6] Sample, I., 2019. What is facial recognition - and how sinister is it? [online] Available at: https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it [Accessed 2 January 2020].

[7] Kharkovyna, O., 2019. An Intro to Deep Learning for Face Recognition. [online] Available at: https://towardsdatascience.com/an-intro-to-deep-learning-for-face-recognition-aa8dfbbc51fb [Accessed 2 January 2020].

[8] Maheshkara,V., Agarwalb, s., Srivastavac, V. K. and Maheshkard, M., 2012. Face Recognition using Geometric Measurements, Directional Edges and Directional Multiresolution Information. Procedia Technology, 6, pp.939-946.

[9] Doffman, Z., 2018. Why Facial Recognition In Schools Seems To Be An Aimless Recipe For Disaster. [online] Available at: https://www.forbes.com/sites/zakdoffman/2018/11/07/why-facial-recognition-in-schools-seems-to-be-an-aimless-recipe-for-disaster/#607f9e601a83 [Accessed 2 January 2020].

[10] Graf, N., 2018. A majority of U.S. teens fear a shooting could happen at their school, and most parents share their concern [online] Available at: https://www.pewresearch.org/fact-tank/2018/04/18/a-majority-of-u-s-teens-fear-a-shooting-could-happen-at-their-school-and-most-parents-share-their-concern/ [Accessed 2 January 2020].

[11] Vance, M., 2018. Official Website of SAFR. [online] Available at: https://safr.com/k12/ [Accessed 2 January 2020].

[12] Lukas, S., Mitre, A. R., Desanti, R. I. and Krisnadi, D., 2016. Student Attendance System in Classroom Using Face Recognition Technique. 2016 International Conference on Information and Communication Technology Convergence (ICTC). Jeju, South Korea 19-21 October 2016. Belgium: EEEI.

[13] Kimaldi, 2019. You are here: Home / Solutions / Access Control / School Time & Attendance control using face recognition terminals[online] Available at: https://www.heraldsun.com.au/business/melbourne-startup-looplearn-scores-470k-for-school-roll-facial-recognition-technology/news-story/7af4c2455842f33afdeb469224a1c636 [Accessed 29 December 2019].

[14] Lim, J., 2019. This Malaysian university will use facial recognition to track students' attendance. [online] Available at: https://sea.mashable.com/tech/4676/this-malaysian-university-will-use-facial-recognition-to-track-students-attendance [Accessed 29 December 2019].

[15] Dewan, M., Akber, A., Murshed, M., and Lin, F., 2019. Engagement Detection in Online Learning: A Review. Smart Learning Environments, 6 (1), pp.1-26.

[16] Connor, N., 2018. Chinese school uses facial recognition to monitor student attention in class. [online] Available at: https://www.telegraph.co.uk/news/2018/05/17/chinese-school-uses-facial-recognition-monitor-student-attention/ [Accessed 29 December 2019].

[17] Alba, D., 2019. The First Public Schools in The US Will Start Using Facial Recognition Next Week. [online] Available at: https://www.buzzfeednews.com/article/daveyalba/lockport-schools-facial-recognition-pilot-aegis [Accessed 29 December 2019].

[18] Carter, M., 2019. Lockport Schools pull faces from facial recognition system; will only track guns. [online] Available at: https://www.wkbw.com/news/i-team/i-team-lockport-schools-pull-faces-from-facial-recognition-system-will-only-track-guns [Accessed 29 December 2019].

[19] Durkin, E., 2019. New York school district's facial recognition system sparks privacy fears. [online] Available at: https://www.theguardian.com/technology/2019/may/31/facial-recognition-school-new-york-privacy-fears [Accessed 29 December 2019].

[20] Kaur, H. and Marco, T., 2019. Durkin, E., 2019. New York school district's facial recognition system sparks privacy fears. [online] Available at: https://edition.cnn.com/2019/05/30/us/ny-school-facial-recognition-trnd/index.html [Accessed 29 December 2019].

[21] Prohaska, T. J., 2019. Education Department bars Lockport schools from testing facial recognition. [online] Available at: https://buffalonews.com/2019/06/28/education-department-bars-lockport-schools-from-testing-facial-recognition/ [Accessed 29 December 2019].

[22] Wu, 2018. High School in China Installs Facial Recognition Cameras to Monitor Students' Attentiveness. [online] Available at: https://www.theepochtimes.com/high-school-in-china-installs-facial-recognition-cameras-to-monitor-students-attentiveness_2526662.html [Accessed 26 December 2019].

[23] Cai, 2017. China's Most Crowded School Has 113 Children Per Classroom. [online] Available at: http://www.sixthtone.com/news/1000089/chinas-most-understaffed-school-has-113-children-class [Accessed 26 December 2019].

[24] Department for Education, 2019. Schools, pupils and their characteristics: January 2019. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/812539/Schools_Pupils_and_their_Characteristics_2019_Main_Text.pdf [Accessed 26 December 2019].

[25] BBC News, 2019. China to curb facial recognition and apps in schools. [online] Available at: https://www.bbc.co.uk/news/world-asia-49608459 [Accessed 26 December 2019].

[26] Feng, 2019. China To Curb Facial Recognition Technology In Schools. [online] Available at: https://supchina.com/2019/09/05/china-to-curb-facial-recognition-technology-in-schools/ [Accessed 26 December 2019].

[27] Barocas, S. and Selbst, A. D., 2016. Big Data's Disparate Impact. California Law Review, 104(3), pp.671.

[28] Information Commissioner's Office, 2019. ICO investigation into how the police use facial recognition technology in public places [report]. Available at: https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf [Accessed 2 January 2020].

[29] Crawford, K., 2019. Regulate facial-recognition technology. NATURE, 572(2), pp.565.

[30] The Biometrics and Forensics Ethics Group, 2019, Ethical issues arising from the police use of live facial recognition technology. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf [Accessed 26 December 2019].

[31] Simonite, T., 2019. The Best Algorithms Struggle to Recognize Black Faces Equally. [online] Available at: https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/ [Accessed 26 December 2019].

[32] Booth, R., 2019. Police face calls to end use of facial recognition software. [online] Available at: https://www.theguardian.com/technology/2019/jul/03/police-face-calls-to-end-use-of-facial-recognition-software [Accessed 26 December 2019].

[33] Campolo, A., Sanfilippo, M., Whittaker, M.and Crawford, K., 2017. AI Now 2017 report. New York: AI Now Institute at New York University.

[34] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., and Floridi, L., 2016. The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2). doi: 10.1177/2053951716679679.

[35] Henry, N. and Powell, A., 2015. Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence. Violence Against Women, 21(6), pp. 758-779.

[36] Harris, J., 2011. School surveillance: how big brother spies on pupils. [online] Available at: https://www.theguardian.com/uk/2011/jun/09/schools-surveillance-spying-on-pupils [Accessed 26 December 2019].

[37] Fuentes, A., 2018. A Brief History of School Violence in the United States (2011). [online] Available at: https://www.versobooks.com/blogs/3705-a-brief-history-of-school-violence-in-the-united-states-2011 [Accessed 26 December 2019].

[38] Poster, M., 1990 The Mode of Information. Cambridge: Polity Press.

[39] Mathiesen, T., 1997. The Viewer Society: Michel Foucault's `Panopticon' Revisited. Theoretical Criminology, 1(2), pp. 215–234.

[40] Xu L., Jiang C., Qian Y., Ren Y., 2018. The Conflict Between Big Data and Individual Privacy. Data Privacy Games. Springer, pp.1-23.

[41] Rejman-Greene, M., 2005. Privacy Issues in the Application of Biometrics: a European Perspective. In: Wayman J., Jain A., Maltoni D. and Maio D, eds. Biometric Systems. London: Springer. pp 335-359.

[42] The New York State Senate, 2019. "Assembly Bill A6787B". [online] Available at: https://www.nysenate.gov/legislation/bills/2019/a6787 [Accessed 26 December 2019].

[43] Maharrey, M., 2019. New York Assembly Passes Bill to Ban Facial Recognition in Schools. [online] Available at: https://blog.tenthamendmentcenter.com/2019/06/new-york-assembly-passes-bill-to-ban-facial-recognition-schools/ [Accessed 26 December 2019].

[44] Beijing AI Principles, 2019. Beijing AI Principles. [online] Available at: https://www.baai.ac.cn/blog/beijing-ai-principles [Accessed 28 December 2019].