Grace Patel
April 11, 2021

Considering the Use of Facial Recognition Technology in Higher Education

I. Introduction

Emerging technologies such as Artificial Intelligence (AI), Virtual Reality, Internet of Things, Quantum Computing, Machine Learning (ML), etc. continue to be a point of focus in the tech industry, but a discussion around policy and regulation must sufficiently occur before the technologies integrate into various areas of our society. AI/ML breakthroughs allowed the development of Facial Recognition (FR) technology to advance to a level deemed adequate for use. While FR technology is already used in handheld devices, airports, businesses, law enforcement, in lieu of passwords, and more, Facial Recognition technology in the US Higher Education System has yet to become the center of attention in the FR discussion. This paper will provide background on the basics of FR technology and its current uses before diving into the use of the technology in various educational modalities and throughout college campus facilities. While investigating the benefits and risk of implementing FR in higher education, several case studies are included to demonstrate the risk of racial bias in FR technology and the current usage of Higher Education FR technology outside of the United States. Because FR is intertwined with privacy concerns, racial bias, inaccuracies, and general mistrust, the implementation of FR technology in higher education must be critically analyzed and paired with a robust risk mitigation strategy. A few core concepts of the risk mitigation strategy provide the foundational concepts to approach the idea of introducing FR technology into the higher education system.

II. Technology Background

In order to consider the positive and negative implications of FR technology, it is necessary to understand how the technology functions and its areas of application. This section will provide an overview of how FR technology processes images and outputs a result, in addition to a few FR technology applications outside of Higher Education.

A. How it Works

FR uses technology to identify a unique human individual based upon their face. By incorporating an image capturing device and other sensors or using existing images or video, a FR system processes an image to classify a face with an existing facial profile that may be labeled as a specific individual. The system uses biometrics to map facial features that comprise a facial signature or “face print”, which is ideally unique to every person. Biometrics can include distance between facial features and other mathematically calculated algorithmic factors, skin texture analysis, 3D imaging to capture face shape, or thermal analysis for situations where hats, glasses, masks, etc. may be preventing a direct visual image of the face (Saravanan, n.d.-a). Most systems use a combination of these techniques to create an image feature set, which is then compared with existing feature sets in a database to search for a potential match. The feature set can also be processed through other algorithms that classify the set’s reaction type or emotion (Symanovich, 2019).

FR systems function differently with varying degrees of accuracy because each system’s algorithm is uniquely constructed to define and weigh the features of an image that construct the facial signature. Some algorithms will return a single match result to a profile in a database, while others will return a list of potential matches ranked with a confidence score, an estimation

of accuracy. Lack of certainty stems from low quality image input, inadequate data points, or poorly-designed algorithms. These error inducing factors produce false negatives and false positives in the FR system, that, if ignored, can be extremely problematic. False negatives occur when the database contains the facial signature of the person in the image being compared, but the algorithm reports no matches between the image's facial signature and the database of facial signatures. False positives arise when the FR system reports an incorrect match between the facial signature being analyzed and a profile in the database. Depending on the application of the FR technology, false negatives or false positives may be a greater risk (Electronic Frontier Foundation, 2020). A case will be discussed in a later section that provides an example for the detrimental and problematic application of a FR system with false positives.

B. Areas of Use

While FR technology may seem like a futuristic notion that threatens our privacy, it is already widely used in a number of areas. According to a Georgetown University Center on Privacy and Technology study, 117 million Americans, about half of all American adults, have their images stored in one or more FR databases that are available to law enforcement agencies (Georgetown Law Center on Privacy & Technology, 2016). Other government agencies, such as the DHS, use FR technology at some airports to identify individuals who have overstayed their visas or are suspected or convicted of a crime. The Washington Dulles International Airport customs officials made their first arrest using FR technology in 2018; they successfully used the technology to catch an imposter attempting to enter the country (Symanovich, 2019).

Businesses have also experimented with FR technology for physical security of their company buildings, with checkpoints at entrances and restricted zones, in addition to creating dynamic marketing tactics based on the audience. For example, FR technology could inform marketing strategy at a concert based on the demographic or for a specific billboard based on who is looking at it. Retailers in stores use FR technology to scan shoppers' faces while in the store and detect suspicious activity. This is not profiling types of people that are generally happier, for example, but rather an analysis of the emotion and responses observed on the faces of individuals based on previous examples of emotional expression. Because the diversity of input data for algorithm training may be imbalanced or of inadequate quality and scale, it is subject to algorithm bias. Social media companies and platforms also use the technology to create suggestions for tagging people in photos, for example. Perhaps the most prevalent use of FR technology is in newer iPhones that have the option of using Face ID authentication to unlock the device. Apple's facial sensor reads the face by projecting 30,000 infrared dots onto the face and then reading its patterns (Saravanan, n.d.-a). The patterns are analyzed by a processor in the iPhone to check for a match with the owner's feature dataset.

The technology is not just proprietary to specific corporations and government entities, but is publicly available, most often as a cloud service from one of the big providers. Facebook Deep face is a 9-layer neural network for training and classifying faces based on photos posted on the platform (Taigman et al., 2014). Google Vision on the Google Cloud Platform and Amazon Rekognition on the Amazon Web Services Cloud Platform offer similar services for their users to process facial data (Amazon, n.d.; Google Cloud, n.d.; Saravanan, n.d.-a). The variance in each platform stems from the identified features, algorithm for processing, and the size/scale of the cross-checked database. Each unique face functions like a uniquely identifiable thumbprint that can also speak through verbal and non-verbal data (Saravanan, n.d.-a).

III. Benefits

Implementing FR in an educational setting could bring about a number of benefits that has the potential to create efficiencies and provide students a more engaging, customized, and secure learning and campus experience.

A. Outside the Classroom

Efficiencies could be created in food service processes and building access on campus grounds for universities. The food services on campus range from buffet-style dining halls, to massive fast food chains and local businesses. The common thread through each of these food service modalities is the need to either identify the individual and/or complete a payment transaction. At some institutions, students may be a part of a food plan that allows access to a buffet-style food service. For Duke University, first-year students have a meal plan that enables an ID card "swipe" to gain access into a dining hall for an all-you-can-eat experience (*First-Year Dining Program*, 2020). Integrating FR technology would eliminate the extra labor and wait time incurred by the manual identification process that is currently required for entry. While this creates efficiencies and students would no longer need to carry a "Duke Card", in the case of Duke University first-year students, it should be noted that this eliminates jobs and poses other risks, which will be discussed later.

For schools that have a more traditional food service structure that emulates individual restaurants, the identification of the customer is less of a priority than the payment process. However, in these situations, FR technology can be used for identification to verify the payment and complete the transaction. A student would order their food as usual and instead of pulling out a card or even paying with Apple Pay, which requires a mobile device, the student would have their face scanned in order to indicate their consent to pay for the food. In China, FR payment (FRP) is already being used and presents itself as more efficient than QR-scanning payments or Mobile-pay (Liu, 2020). However, non-intuitive FRP platform onboarding processes have led to mistrust with FRP. A similar US trial exists in food service establishments in Los Angeles, CA (Dean, 2020). Although they are not without issue, China and LA show a proof of concept for using FRP with food establishments that could create similar benefits and efficiencies in payments on university campuses.

Additionally, the technology could be used to create greater security for students, dorm buildings, ideas, and research. Most college campuses require some form of identification or key in order to allow entrance to campus facilities, like dorms, classrooms, gyms, and labs. In lieu of a passcode, card swipe or card tap, a FR system could identify individuals and determine if they are allowed to enter the building. An FR system would be more secure with regards to building access because stolen phones or cards could not be used to gain entry. However, this may also inconvenience many students who may have guests in their dorm, give a tour to family friends, or ask friends to retrieve something on their behalf. Using FR technology for building access management could replace and improve current security measures.

FR for identity authentication may prove to be more beneficial in a remote setting than for physical security access. With the rise of the cloud and mobile devices, there exists an increasing number of transactions and amount of data online (Blue Line Technology, n.d.). Educational institutions must adapt to allow students, faculty, and staff to immediately access their accounts, systems, and information from any location or device without compromising the security of the data and infrastructure (Secure Access for Higher Ed, n.d.). Due to the COVID-19 Pandemic, 90% of American colleges and universities have experience some shift towards virtual learning,

and if the trend towards virtual learning persists, as many predict, the need for secure remote access will be of widespread importance for students (Inside HigherEd & Lederman, 2020). Campuses have addressed remote security of sensitive research, access to IT services and email, and businesses critical systems like finance, HR, or IT administration access through implementing Multi-Factor Authentication (MFA) protections (Lewis, 2019). MFA verifies the identity and access permissions of a user with more than one method or key that usually falls into one of three categories: informational keys, physical keys, and biometric features. These three cornerstones of authentication are commonly known in the cybersecurity industry as "something you know, something you have, and something you are" (NIST, 2017). As previously discussed, informational keys, such as a passcode, and physical keys, such as a fob or card, are much easier to replicate or produce than a set of biometric features that are uniquely identifiable to an individual (Blue Line Technology, n.d.). Using MFA with facial feature authentication would support the existing MFA security goals of educational institutions to a greater degree of security. FR technology with MFA could provide an efficacious addition to remote identification and authentication.

B. Inside the Classroom

More insightful implementations of FR in the classroom could provide data to improve student learning experiences and create a more impactful learning environment. Some FR technology has been developed to recognize a wide range of nonverbal expressions and emotions. Similar to the use of facial mapping features to match faces to facial signature profiles, FR algorithms can also be tuned to recognize feature sets common to particular sentiments and emotions. Collecting facial imaging data during a lecture could be used with FR technology to create data for professors after a lecture about student engagement. Understanding which parts of a lecture were most or least exciting and parts of the lecture where students paid the most or least attention brings new insights for specific content communication and effective teaching practices. At a higher level, the technology could generate datasets about how students learn, effectiveness of different methods of learning, topics of greatest engagement, and differentiators between great classes/teachers (Saravanan, n.d.-b).

In addition to individual class improvements and overall insights about learning styles and teaching methodologies, data could be aggregated for an individual and given directly to students about their learning strengths or weaknesses and their preferred learning method based on when they are most engaged, happy, etc. Chegg acknowledges commonly accepted research that identifies three main types of learning methods: auditory, visual, and kinesthetic. FR technology from the classroom could provide a data-driven approach to discovering personal learning styles that surpass the accuracy and effectiveness of online quizzes, such as Chegg's "What type of Learner Are You?" Quiz (Bastian, 2018). Self-understanding around learning promotes impactful educational engagements and better learning outcomes (LA ORT Career College, 2017). These individual learning insights from FR in conjunction with refined teaching methods and content communication could significantly improve levels of education.

In a more logistically oriented approach, FR technology could be used to assist in tracking course attendance, a requirement that some universities still hold. Whether online or in person, the attendance tracking process could be streamlined and automated with FR technology in order to save time.

IV. Risks

Adopting FR technology on higher education campuses creates a number of risks. Concerns with privacy for students, accuracy of the algorithms, racial bias in the algorithms, and public distrust all create hesitancies for implementation. In the section following Risks, recommendations for successful implementation that mitigate these risks are outlined.

A. Privacy

FR technology hinges on the ability to capture face images through surveillance devices and easily determine their identity. The large amount of data collected creates a valuable data set that can be leveraged for tracking in surveillance. The university becomes responsible for the protection and proper usage of the data once it is collected. Due to the possibility of data misusage by the university claiming to protect the data or in the case of stolen data, the privacy of those in the FR database is vulnerable. If the privacy of the FR systems on campus are breached, student likeness could be compromised, or hackers then have access to student data.

Longevity of the FR database creates an increasing risk as the system collects more data over time. The valuable data becomes more comprehensive and attractive to hackers, so universities will need to invest money in building sturdy systems. To ensure that databases are secure from malicious attackers, institutions will need to maintain a secure and large database library of FR data.

While a growing database of a person's identity, data, and safety may cause an increasing threat from hackers, there also remains a privacy concern with the university. The learning algorithm in conjunction with the facial signature database allows the university to identify students in any sort of media available openly on the internet. Any photos or videos from campus surveillance, in addition to any public social media visual content and accessible online imagery could be scanned and matched with a student or faculty profile. Privacy on and off campus would cease, as the university would have the power to track any individual with an adequate sampling of data in the FR database.

B. Accuracy

Institutions will use systems with varying degrees of accuracy that are either proprietary or from an outside company. A few of the most notable private FR software companies include Deep Vision AI, SenseTime, FaceFirst, TrueFace, and Clearview AI (Analytics Insight). With ideal lighting and positioning conditions and some of the top algorithms determined by the NIST Facial Recognition Vendor Test, like the one developed by Vision Labs, can reach accuracy scores of above 99.9% (*FRVT 1:1 Verification*, 2020). However, many algorithms produce much less accurate results and are impacted by environmental factors in images such as non-direct angles, masks, glasses, blurry captures, and shadows. Through the NIST Facial Recognition Vendor test, it was also concluded that age also impacts error rates. Images of an individual from many years ago may not produce the same face-print as a current facial image (Crumpler, 2020).

Universities will need to operate and maintain the devices for capturing and processing facial imagery to ensure smooth functioning and accuracy (Grother et al., 2017). Additionally, the accuracy for FR algorithms may be different for different demographics. Generally, the software has been shown to be less accurate for children and young adults in addition to women (Buolamwini & Gebru, 2018; Burke, 2020). Inaccurate results will yield ineffective systems that will ultimately fail to increase security, incur a large monetary cost, and disproportionately disadvantage certain groups.

C. Racial Bias

While FR algorithms and public platforms produce inaccuracies, there has been a disproportionate rate of error for identification of faces from non-white individuals. A 2018 test conducted by the ACLU found that Amazon's 'Rekognition' FR software falsely matched 28 members of Congress with mugshots of individuals who had been arrested for criminal actions, despite the fact that Amazon had been marketing the software to law enforcement agencies (Snow, 2018). The breakdown of demographics for the misclassified images reveals that people of color were misidentified at twice the rate of normal. 39% of false matches were people of color even though they only make up 20% of congress. The National Institute of Standards and Technology (NIST) conducted a similar study but investigated a broader range of FR systems. The NIST team analyzed 189 FR algorithms designed by 99 different developers and found that when conducting image-to-image comparison, Asian and African American faces had higher false positive rates than Caucasian faces (Meyer, 2020). However, facial images of American Indian individuals had the highest false positive rate, which is likely due to a lack of training data for minority groups.

Kashmir Hill, a well-established technology journalist with an interest in FR technology, captured Robert Williams's experience with racially biased algorithms, which may be one of the first documented instances of a wrongful arrest made because of faulty FR technology. Williams was arrested on his front lawn in front of his family, then taken to the local station for interrogation before law enforcement realized that he was completely innocent (Hill, 2020). The case was dismissed, but Williams's life was interrupted, and law enforcement did not acknowledge the prejudice of the case. If racial biases go unaddressed for FR implemented on campuses, both people of color and women will experience greater inconvenience, injustice, and danger from being locked out of dorms, misread in the classroom, wrongfully accused by the police or student conduct, marked absent, and denied access to campus facilities (Burke, 2020).

The bias could likely be corrected by providing more data from minority groups to be used for training FR algorithms, however, companies, developers, policy-makers, and the public must first recognize racial bias as an issue. The number of studies conducted and stories shared that reveal racial bias in algorithms have pushed IBM, Amazon, and Microsoft to shut down their FR services for law enforcement, but the services are still available for use by other entities (Heilweil, 2020). While the impact in the Higher Education sphere may not be as direct as false accusations and arrests for crime, the issues created by the bias in an educational environment still persist. In a letter, the Congressional Black Caucus urged Amazon CEO, Jeff Bezos, to urgently improve the inaccuracies and disproportionate inaccuracies for people of color in FR (Richmond, 2018). Implementing FR technology throughout campus without addressing algorithm bias would further exacerbate disadvantages for people of color.

D. Moratoriums and Opposition

As mentioned, the implementation of FR technology has been seen across a wide number of industries, including education. In 2019, the New York school district of Lockport began a program to pilot the use of FR technology for campus security (Alba, 2019). Not only did the New York State Education Department direct the district to postpone the program, but also the Future of Privacy Forum (FPF) wrote a letter to the NY State Legislature supporting a moratorium on FR use in public schools – both K12 and higher education (Vance, 2019). The FPF highlighted the danger of proceeding with such a pilot without full definition of regulations and also asserted recommendations to the school district.

Most directly, the FPF recommended that the Lockport school district, and any school district, avoid the use of FR tech in public school facilities until a comprehensive study of its impact on education systems is completed. Proceeding without full knowledge of the impacts could both introduce new issues and undermine the positive use of biometric data. Many schools already use non-facial biometric data, like fingerprints and handprints, for school functions, and facial biometric data to assist special education, occupational therapy, and physical therapy initiatives (Vance, 2019).

The FPF would allow existing systems that leverage non-facial biometric data to continue operating and carefully construct policy language to protect programs that benefit those with disabilities. Only after comprehensive studies prove that FR tech increases school safety and the benefits outweigh the risk and costs of purchase, implementation, training, and maintenance can the implementation of FR technology be considered. If the technology integrates into schools, it will require explicit and early communication in addition to consent of all individuals involved.

The backlash that the Lockport district experienced when announcing the launch of the FR program is not an isolated incident. UCLA announced a proposal to implement FR technology on campus and received backlash from the student body and other stakeholders. Alongside a national digital rights advocacy organization called Fight for the Future, students voiced opposition to having their data captured and stored.

After the backlash and a study showing that FR software, specifically Amazon's, was highly inaccurate, UCLA dropped their plan publicly. The backlash at UCLA occurred despite over-the-table administrative strategy and allowance for a comment period. However, there is no policy requiring private universities to openly declare their use of FR technology, which means some institutions may be using FR technology with no regulation or disclosure. Schools were likely dissuaded from introducing FR on campus because of the UCLA plan failure, despite efforts from FR companies who market to universities (Burke, 2020). Ultimately, more policies need to be put in place that, at a minimum, require institutions to disclose their actions, and once further direction is defined, does not leave security and regulation to the discretion of school administrators.

V. Successful Implementation

Due to a large number of risks and doubts about the significance of FR benefits, successful implementation will hinge on a carefully timed strategy aligned with the development of accurate technology and an open attitude from the public and stakeholders within the higher education system. As seen with the implementation of FR technology in law enforcement, lack of transparency and regulation can foster ill-sentiment and refusal of services from big tech companies like IBM, Amazon and Microsoft (Heilweil, 2020). Addressing planning, security, and autonomy in advance will lead to a higher likelihood of implementation success.

A. Planning and Foresight

While there are a few key components that are necessary for the safe and successful adoption of FR technology in a higher education setting, the top principle is early planning and a critically developed vision. As addressed in the former part of this paper, FR technology cannot be treated lightly or as a fun, new administrative toy. Successful implementation necessitates a safe implementation, which requires a well thought out practical plan that encompasses transparency and safety.

As an institution begins to develop a plan, the team will need to solicit the help of FR technology, education, personal relations, policy, and marketing experts. Every aspect of the new system and implementation needs to be thought through and documented, especially considering the backlash that other institutions have previously received. Technologists will help consider the competency of the system and privacy concerns. Educators will best define the uses for the technology and define policies with policy-makers around the system. Marketing experts will spearhead clear and comprehensive communication to the student body, parents, faculty, and staff, while the personal relations experts will communicate with the media. A student perspective will also be extremely valuable in this interdisciplinary, multi-stakeholder initiative. Drawing on the collective experience and expertise of the planning team, greater clarity will be reached on the practicality of a secure, consensus-driven, net beneficial FR system for a college campus.

If a solution or plan is reached, the details will include answers to questions such as: How many cameras? Where will cameras be placed? How will the university create clear communication and expectations with the public? What are the response procedures for compromise of a single identity and/or the whole system? How will our system's success or failure affect the overall FR technology conversation and the culture at other universities around technological implementation? What regulations need to be addressed? How do we ease student, faculty, and stakeholders' concerns?

B. Security

The equipment and physical setup need to be secured and thoroughly tested to ensure maximized accuracy and minimized errors. When there is an error, a remediation plan will need to be established so that clear proceedings following the error will keep things running smoothly with minimal harm to the user. Additionally, systems must be able to identify any user fraud that may occur such as criminal attempts to recreate the likeness of a student through masks or 3D images generated from public media (Saravanan, n.d.-b).

The overall system must offer alternative solutions for instances when the FR technology malfunctions and also create a conflict-resolution process for system errors. As an example, it is dangerous for a student to be locked out of their dorm late at night, and there must be an alternative method for a student to gain access to their building. A solution to ensure a more accurate identification system, and hence less malfunction, is to develop a robust and highly accurate database. Perhaps students have visibility into the images of themselves in the school's database. When a student realizes that an image in the school's database had been incorrectly identified to their profile, a formal procedure could allow the student to correct their set of data points in the database. A similar set-up could exist for attendance tracking, which would allow students to adjust their attendance, upon approval, in the instance that the FR system failed to record their attendance correctly (Saravanan, n.d.-b).

For maximum security, the stored face prints must use a specific database solely for the use of FR, and the data should be encrypted. The privacy of the data stored for the FR system should not intertwine with any other student data or data tied to the institution, which is why it must operate on its own servers. Access management of the data should be defined by education, cyber, and policy experts to determine the ability of IT, advisors, faculty, students, and parents to view any (or none) of the data gleaned from the system. Further, encrypting the data will help preserve the privacy of each individual and a system could be designed so that compute locations

are able to determine an identification conclusion without sharing information (Erkin et al., 2009).

The pieces involved in the technology system include the image capturing device, algorithm, and database, all of which need their relationships with one another to be defined. A system can be set up to communicate and transfer data in a number of different ways, one of the most recently popular methods being the cloud. Using the cloud implies that there are designated servers or encrypted virtual machines for the FR technology to be used for the system's purposes, such as storage of the facial image dataset, computation of features on new images, and running algorithms, which then send information over the internet. Edge computing redistributes storage and computational tasks for a system by localizing data at a number of smaller, spread out servers. Computing on the Edge creates computational speed benefits that are greatest when cloud servers are thousands of miles away. Additionally, computing on the Edge is more computationally efficient, reduces connectivity cost, and opens the opportunity to localize data (RCN Business, n.d.). However, Edge-heavy computing for FR in higher education places computational responsibility at the camera location, which may be difficult to achieve because it is necessary to access the facial database in order to come to an identification conclusion. Also, the new image will likely need to be added to the existing data set and will be sent across the network anyways. A 2019 study of 270 IT decision makers by Kollective, an Oregon based cloud company, found that 66% of IT teams view Edge computing as a threat to organizations (Bayern, 2019). Adding more end-points to a system increases the points of vulnerability, and it would significantly increase the vulnerability of the dataset if every Edge location had access to the entire facial dataset.

Some computation on the Edge may benefit a higher education FR system for security purposes by decreasing the amount of data actually stored in the system. The image capturing devices act as Edge locations that could compute the biometric face-print locally and send the data to the central server without transferring the whole image. In this scenario, for example, the amount of stored data is limited, and the end points do not need to store any data, which decreases vulnerability. From a speed perspective, which also relates to overall safety and well-being of students, an Edge based approach would create significant improvement of the system's latency because the information only has to travel within a college campus, which are relatively small in size compared to the distances covered by cloud computing systems that utilize the Edge today (*Global Infrastructure Regions & AZs*, n.d.).

C. Communication and Autonomy

Educational Institutions should prepare students, faculty, and other stakeholders for the introduction of FR with no surprises and the ability to remove themselves from the system. An institution must establish clear grounds and intentions for the use of the data and each application it plans to pursue. In order to avoid a culture of surveillance, technology use will be limited to its documented and communicated purposes (Saravanan, n.d.-b). Communication with stakeholders does not stop after the announcement of the initial plan, but rather as the plan evolves and incidents occur and are remediated, all persons involved should be informed.

Facebook, Google, and the California Consumer Privacy Act (CCPA) champion the concept of consumer-controlled privacy and consent to systems employing FR technology. Facebook automatically turns on FR for tagging suggestions of faces in photos, but a user has the option to opt-out of the suggestion feature. Similarly, Google+ allows their users control, but through an opt-in option for their FR technology that can be turned on and off at any point

(Symanovich, 2019). The CCPA gives California residents more agency over the effective use of their data by enabling more control for users to delete their data stored in a company database. The same principle of agency and autonomy should be enabled in a higher education FR system. Opt-in/opt-out models will work well for things like classroom learning style identification, but the challenge of initiating consent for campus-wide building security is more nuanced. If individuals refuse to have their facial data stored, their identity cannot be confirmed through FR, and they will need an alternative security verification for entry.

VI. Policy in Practice

A. US Policy

Much of the FR technology in the US has operated without any sort of official regulation. Policy can be put in place at a company, local, state, and federal level, however, very few laws exist that address biometric data. The standards and practices in industry largely come from best practices, guidelines, and recommendations publications by associations and groups adjacent to tech policy such as the International Biometrics and Identification Association, the IEEE Stands Association, The Digital Signage Federation, the U.S. Chamber of Commerce, and the Federal Trade Commission (FTC) (Greenberg, 2020). In the FTC's "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies" Staff Report, the recommendations broadly advocate for designing with consumer privacy in mind, establishing reasonable security and process for determining which data to retain, communicating to consumers, and maintaining sensitivity of information (Federal Trade Commission, 2012).

As mentioned before, the CCPA introduces more consumer agency over their data and allows consumers to request removal of their biometric data held by any company. Several other states have introduced biometric data into their existing personal information and security breach laws, but the policy for biometric data, privacy, and FR remains scattered (Greenberg, 2020). As FR technology develops, more commercial applications of FR arise and discussion over California and Europe's privacy laws increase, lawmakers may turn attention to federal privacy legislation that encompasses the commercial use of FR technology.

B. School in China

China's approach to FR technology has been much more lenient on privacy policy and implementation, which has led to an earlier and wider spread use of the technology. In early 2017, Beijing Normal University in China implemented a facial and voice recognition entry system in a female dormitory as a pilot to test the system and to prohibit non-residents from entering the building (Connor, 2017). Upon the success of the pilot, the University planned to install the scanners and FR systems in nine other female dormitories during the same year in order to increase the scale of the trial.

Students register by taking photos of themselves from various angles, similar to the process of setting up "finger scan" on an iPhone to create a thumbprint profile that is stored on the device. From the initial set of photos (and voice recording sample), the system allows or denies access to individuals, sounds an alarm if the facial or vocal prompt is not recognized and notifies the university if a student does not return to the dorm within 24 hours, which prevents intruders, increases safety, reduces staff, and prevents dorm lockout from missing or forgotten keys (Chen, 2017).

After the Spring trial, the next school year in September began with new student facial scans for a campus-wide FR system (Chen, 2017). The school is operating under the Cybersecurity Law of the People Republic of China which lays out the law for the protection, use, and collection of biometrics and other personally identifiable information (PPI) (Lee, 2020). An update to the Law came into effect in March 2020 which introduced modifications to strengthen the policy by increasing privacy protection and altering the "exceptions to soliciting consent" clauses.

VII. Conclusion

Introducing Facial Recognition in higher education poses a new technology and policy challenge for the United States. While FR could be used inside the classroom to inform more impactful and effective learning experiences and outside the classroom to increase building and payment security and efficiency, the current risk with privacy for students, accuracy of the algorithms, racial bias in the algorithms, and public distrust signal that FR cannot be implemented until the aforementioned are addressed.

A cost-benefit analysis and trials with small audiences and a few dorms or select number of classes can be conducted until comprehensive understanding of the implication of FR for higher education is reached. Through transparent communication and a multidisciplinary effort, new FR systems and policy may be defined that comply with emerging privacy policy at a state and federal level. Solidifying a strategy to carefully implement FR in higher education without creating undue risks for students and other stakeholders will mark a new era of privacy policy, trust, and technology benefits throughout education and security.

References

Alba, D. (2019, May 30). *Lockport Public Schools Will Be The First In The Country To Use Facial Recognition On June 3*. BuzzFeed News. https://www.buzzfeednews.com/article/daveyalba/lockport-schools-facial-recognition-pilot-aegis

Amazon. (n.d.). *Amazon Rekognition*. Amazon Web Services, Inc. Retrieved November 15, 2020, from https://aws.amazon.com/rekognition/?blog-cards.sort-by=item.additionalFields.createdDate&blog-cards.sort-order=desc

Analytics Insight. (2019, November 29). *Best Facial Recognition Software*. https://www.analyticsinsight.net/best-facial-recognition-software/

Bastian, F. S. (2018, February 5). *Quiz: What Type Of Learner Are You?* Chegg. https://www.chegg.com/play/student-life/quiz-what-type-of-learner-are-you/

Bayern, M. (2019, October 18). *66% of IT teams view edge computing as a threat to organizations*. TechRepublic. https://www.techrepublic.com/article/66-of-it-teams-view-edge-computing-as-a-threat-to-organizations/

Blue Line Technology. (n.d.). *Two Factor (2FA) with Facial Recognition*. http://bluelinetechnology.com/wp-content/uploads/page/500/white-paper_two-factor.pdf

Buolamwini, J., & Gebru, T. (2018). *Gender Shades*. Proceedings of Machine Learning Research. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Burke, L. (2020, February 21). *UCLA drops plan to use facial recognition security surveillance, but*. Inside Higher Ed. https://www.insidehighered.com/news/2020/02/21/ucla-drops-plan-use-facial-recognition-security-surveillance-other-colleges-may-be

Chen, L. (2017, September 4). *Student face and voice scans the new keys to Chinese university dorms*. South China Morning Post. https://www.scmp.com/news/china/society/article/2109640/chinese-university-tells-students-use-voice-and-facial

Connor, N. (2017, May 16). *Facial recognition installed in female university dormitory in China – to Keep Out 'Strangers.'* The Telegraph. https://www.telegraph.co.uk/news/2017/05/16/facial-recognition-installed-female-university-dormitory-china/

Crumpler, W. (2020, April 14). *How Accurate are Facial Recognition Systems – and Why Does It Matter?* Center for Strategic and International Studies. https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter#:%7E:text=In%20ideal%20conditions%2C%20facial%20recognition,Recognition%20Vendor%20Test%20(FRVT)

Dean, S. (2020, August 14). *Facial recognition payment tech is rolled out in L.A. area*. Los Angeles Times. https://www.latimes.com/business/technology/story/2020-08-14/facial-recognition-payment-technology#:%7E:text=As%20so%2Dcalled%20contactless%20payments,Chicken%20Shack%20and%20regional%20chains

Electronic Frontier Foundation. (2020, August 25). *Face Recognition*. EFF. https://www.eff.org/pages/face-

recognition#:%7E:text=Face%20recognition%20systems%20use%20computer,in%20a%20face%20recognition%20database

Erkin Z., Franz M., Guajardo J., Katzenbeisser S., Lagendijk I., Toft T. (2009)

Privacy-Preserving Face Recognition. In: Goldberg I., Atallah M.J. (eds) Privacy

Enhancing Technologies. PETS 2009. Lecture Notes in Computer Science, vol 5672. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-03168-7_14

First-Year Dining Program. (2020). Duke Blue Book. https://bluebook.duke.edu/first-year-students/living/dining/first-year-dining-program/

FRVT 1:1 Verification. (2020, September 18). NIST. https://pages.nist.gov/frvt/html/frvt11.html#overview

FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies. (2012, October 22). Federal Trade Commission. https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition

Georgetown Law Center on Privacy & Technology. (2016, October). *Unregulated Police Face Recognition in America*. The Perpetual Line Up. https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf

Global Infrastructure Regions & AZs. (n.d.). Amazon Web Services, Inc. Retrieved November 9, 2020, from https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Google Cloud. (n.d.). *Vision AI*. Retrieved November 15, 2020, from https://cloud.google.com/vision

Greenberg, P. (2020, August 18). *Facial Recognition Gaining Measured Acceptance*. National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measured-acceptance-magazine2020.aspx#:%7E:text=No%20federal%20laws%20address%20commercial,protections%20in%20place%20for%20consumers.&text=Other%20state%20laws%20require%20businesses,including%20biometric%20data%2C%20they%20hold

Grother, P., Quinn, G., & Ngan, M. (2017, March). *Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8173

Heilweil, R. (2020, June 11). *Amazon, IBM, and Microsoft back away from selling facial recognition to police*. Vox. https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

Hill, K. (2020, June 24). *Wrongfully Accused by an Algorithm*. The New York Times. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Inside HigherEd, & Lederman, D. (2020, April 22). *How Teaching Changed in the (Forced) Shift to Remote Learning*. Inside Higher Ed. https://www.insidehighered.com/digital-learning/article/2020/04/22/how-professors-changed-their-teaching-springs-shift-remote

LA ORT Career College. (2017, February 2). *Benefits of Finding Your Learning Preference*. Los Angeles ORT College. https://www.laort.edu/benefits-finding-learning-

preference/#:%7E:text=Knowing%20your%20learning%20style%20can,lessons%20%E2%80%93%20how%20to%20learn%20efficiently

Lee, S. (2020, April 4). *Coming into Focus: China's Facial Recognition Regulations*. Center for Strategic and International Studies. https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations#:%7E:text=This%20past%20February%2C%20China%20introduced,a%20slightly%20lower%20accuracy%20rate.&text=In%20October%202019%2C%20China%20had,use%20of%20facial%20recognition%20technology

Lewis, N. (2019, October 9). *Multi-factor Authentication Deployment in Higher Education*. National Cybersecurity Alliance. https://staysafeonline.org/blog/multi-factor-authentication-deployment-higher-education/

Liu, F. (2020, May 10). *Case Study of Facial-Recognition Payment in China*. Nielsen Norman Group. https://www.nngroup.com/articles/face-recognition-pay/

Meyer, C. (2020, May 1). *Facial Recognition Error Rates Vary by Demographic*. ASIS. https://www.asisonline.org/security-management-magazine/articles/2020/05/facial-recognition-error-rates-vary-by-demographic/

National Institute of Standards and Technology (NIST), Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017, June). *NIST SP 800–63-3 Digital Identity Guidelines*. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-63-3

Richmond, C. L. (2018, May). *Letter to Jeffrey Bezos from the Congressional Black Caucus*. Congressional Black Caucus. https://cbc.house.gov/uploadedfiles/final_cbc_amazon_facial_recognition_letter.pdf

Saravanan, R. (n.d.-a). *Facial recognition can give students better service (and security)*. Ellucian. Retrieved October 20, 2020, from https://www.ellucian.com/insights/facial-recognition-can-give-students-better-service-and-security#:%7E:text=On%20college%20campuses%20in%20the,unnecessary%20and%20invasive%20monitoring%20tool

Saravanan, R. (n.d.-b). *How higher ed can prepare for facial recognition*. Ellucian. Retrieved November 10, 2020, from https://www.ellucian.com/insights/how-higher-ed-can-prepare-facial-recognition

Secure Access for Higher Ed. (n.d.). Duo Security. Retrieved February 2, 2021, from https://duo.com/solutions/industry-solutions/education

Snow, J. (2018, July 26). *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*. American Civil Liberties Union. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Symanovich, S. (2019, February 8). *How does facial recognition work?* Norton. https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014, June 24). *DeepFace: Closing the Gap to Human-Level Performance in Face Verification*. Facebook Research. https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/

Vance, A. (2019, June 17). *FPF Letter to NY State Legislature*. Future of Privacy Forum. https://fpf.org/2019/06/17/fpf-letter-to-ny-state-legislature/

What Are The Benefits Of Edge Computing vs. Cloud Computing? (n.d.). RCN Business. Retrieved November 20, 2020, from https://www.rcn.com/business/insights-and-news/insights-articles/edge-computing-vs-cloud-computing/#:%7E:text=Reliable%2C%20uninterrupted%20connection-,Lower%20connectivity%20costs%20and%20better%20security%20practices,for%20you%20and%20your%20customers