Privacy Issues Concerning Biometrics in Grades K-12

Braydon T. Stutzman and Dr. Christopher B. Davison

Ball State University

btstutzman@bsu.edu; cbdavison@bsu.edu

Abstract
Biometrics are a large step forward in securing information and data. With these advancements, there is the desire to implement biometric technology everywhere. In most places, it would be a straightforward implementation, but in K-12 schools it could pose a risk to children's privacy. The biometric information utilized by the school administration could be stolen or used maliciously. Along with the security risks, Family Educational Rights and Privacy Act (FERPA) issues could prevent schools from using the biometrics. The purpose of this paper is to discuss the privacy concerns of biometric technology in a K-12 environment.

Introduction

As a society that adapts to technology improvements, people are always looking for better ways to secure information. Biometrics are an excellent way to keep data safe and out of the hands of cyber criminals. With that extra security comes some potential risks. To be able to use biometrics, a person would need to give the machine a very personal part of their identity (e.g., fingerprints, voice patterns). Doing this prevents others from accessing the same data, but if taken by someone else, would be devastating to the owner. In this article, several biometric technologies and their concomitant issues are explored as they relate to deployment in K-12 schools.

The idea of implementing biometrics in schools is of potential benefit. Added security and personalized access is important for an organization that deals with the development of children. The downside to this would be that the minor's data would be stored by the school. The fingerprints and facial scans would be part of the school's data. This can pose a risk of getting hacked and having access to this personal information. Along with issues in storing the data, parents can opt-out completely. FERPA allows parents to opt-out their children from technologies such as a biometric scan.

Literature Review

With the advancement of computer technology over the last decade, the use of biometrics in authentication has gained much attention. The idea was first introduced in the 1980s when the US was pursuing approaches to tightening drug smuggling from southern borders (Andreas, 2000). Its application then expanded to identifying legal and illegal immigrants in the 1990s (Ceyhan, 2008; Bigo, 2002). After 2000 and with the widespread use of Web-based systems, it has become popular in implementing secure systems.

One noted aspect of biometric security techniques is the lack of susceptibility to standard attacks. Other security measures such as username/password authentication, CAPTCHA, and security questions are more vulnerable to traditional cyber-attacks such as brute force, social engineering,

and dictionary attacks and therefore underperform biometric techniques in authentication (Kowtko, 2014).

Biometric security is considered one of the best options for children and older adults due to its relative ease of use. The number of IT users among older adults is increasing. They use the Internet for a variety of purposes such as access to news sources, telehealth, and E-commerce websites. Given the recent outbreak of COVID-19, a large percentage of students take online classes and therefore use the web to connect to their classes and do their assignments. Regular authentication measures such as username and password, CAPTCHA, and security questions cause confusion for elementary students and as a result will create an unpleasant experience of online learning. Biometric security can facilitate delivering online materials especially in terms of efficient authentication and ease of use. In spite of its potential, there are downsides to biometrics such as implementation cost and security concerns (Kowtko, 2014).

Biometric data is sensitive personal data and its leakage can cause serious risks. It is suggested in several articles that biometric information such as iris, face, handshape, and fingerprint can be reproduced from biometric reference template (JGalbally, 2013) (Adler, 2003) (Gomez-Barrero J.G.-G, 2014) (Cappelli, Maio, Lumini, & Maltoni, 2007). As a result, approaches such as irreversible facial reference, and Bloom filter have been proposed to address the issue (Gomez-Barrero C. R., 2014).

Types of Biometric Technologies

Biometrics are widely popular and easily accessible, but some more than others. There are numerous implementations of biometric systems. The most common and probably most well-known is the fingerprint scan. The fingerprint scan is a visual biometric. It takes the ridges of the finger to determine who is trying to gain access to the information. Another common biometric system is facial recognition. This can be used in CCTV (Closed-Circuit Television) and is used with video surveillance in many places, such as schools. Facial recognition software scans a person's face and identifies traits that only that person has, such as distinct patterns and facial structure. The last common form of biometric is gait. This goes along with facial recognition because it can be used with CCTV. Gait detection is a behavioral biometric. It recognizes the way someone walks and carries themself and determines who that person is without having to see their face.

Privacy Issues

Although biometrics are a large step toward a more secure environment, there are many concomitant privacy concerns (Leaton, 2018) . The first issue is what happens to that data when it is compiled. The data that is taken to use biometrics, is stored somewhere. With that data being stored, there is the potential to have it stolen or misused. The biometric data is extremely personal and can become an issue if it is exploited (especially for minors). Having a liability as serious as minors' privacy can make the implementation of biometrics complicated.

FERPA. FERPA is a privacy act implemented by the US department of education in 1974. This was made to protect minors from privacy issues and moral dilemmas (Frank & Wagner, 2018). An issue that arose before FERPA was a school could student files that they may not be compelled to provide to the parents. When FERP was implemented, parents had more

control of records disclosure. FERPA is an important factor when considering biometrics. Also, FERPA mandates that the parent would need to consent to collect or provide their child's information.

How the UK navigates privacy issues. The United Kingdom has had little issue implementing biometric technology within their schools as they do not have privacy acts as strict as FERPA. The main form of biometric technology used in the UK is fingerprint scanning. Gait recognition and facial recognition are also used within some schools.

Legal Issues Impacting Biometrics

Although FERPA is an issue when trying to implement biometrics in the US, other privacy issues arise with specific states. In the US, some states have biometric privacy regulations, and other states have banned the technology outright. In 2016, the state of Florida decided upon a ban of biometrics in schools because it could pose a privacy risk.

Of the many legal and societal prohibitions, FERA is the largest barrier in implementing biometrics within the US school systems. Although FERPA prevents some schoolwide implementations, another barrier is individual state restrictions. As mentioned before, Florida has a ban on biometrics in schools, but they are not the only state that has made this decision. Maryland has a ban on collecting any biometric data from students that attend public schools in Carroll County (Senate Bill, 855). The bill prohibits any physical collections of biometric data. This includes fingerprints, facial recognition, and vocal characteristics.

US Laws Governing Privacy

The US, comparatively speaking, does have significant privacy legislation as well as FERPA protection. Where other country's schools have liberty over biometric technology adoption, the US does not.

In the US, specific laws that prohibit biometrics from K-12 schools are more statewide than they are countrywide, FERPA notwithstanding. Florida and Maryland both have laws prohibiting biometrics in schools. Legal compliance in protecting the students' data makes the school responsible for any data misuse. Implementing biometrics increases the liability of the school regarding students' privacy and data. Careful research is required in order find biometric services that protect the students' data and are compliant with all applicable legal requirements.

Analysis of Biometric Technologies and Implementations

Biometric devices and technologies can be classified into several implementations. These classifications range from, chemical, visual, behavioral, and auditory. Some examples of these would be DNA matching (chemical), iris recognition (visual), gait detection (behavioral) and voice recognition (auditory) (Biometric Institute, 2018). The most readily implementable biometric technology for most schools would be fingerprint scanning. In some schools, primarily in Europe, the fingerprint scans are used for events such as meals or signing into school (Mayhew, 2015). Another type of biometric technology that is used within schools are vein readers or palm readers. These are used for the same purpose as the fingerprint scanners. However, there are sanitation issues with all the students touching the same device.

For the biometric scanning technology, there exists several categories. The chemical biometrics are DNA matching scans. These are unused in schools and are found more in the medical field. Visual biometrics range from ear scans, eye scans, face scans and fingerprint scans. These are the most popular and are used in some schools. Behavioral scanning is mostly confined to gait detection. This is used in many places paired with CCTV to recognize how someone carries themself. Auditory scans are for voice recognition. This type of technology is used over phones or videos to determine who is talking.

Positive aspects of biometrics. The benefits of biometric systems in any organization are immense. The most well-known and obvious strong suit of using a biometric system is that the data being presented to the device is nearly impossible to spoof or replicate. It also cannot be shared with anyone like a password or a token. Another advantage of using biometrics to an organization is that the user cannot forget or misplace their login information. The information is biologically permanent. Finally, biometrics are significantly more convenient. Without having to remember a password or carry a token, the inconvenience of logging in somewhere is virtually eliminated.

Negative aspects of biometrics. There do exist detriments to the adoption of biometric technology. Chief among those is the fact that even biometrics can still leave an account compromised. The first underlying issue is that if an account gets compromised, there is no way to change the login information. The human body cannot change its information. Fingerprints and facial recognition cannot be changed, even if the account has been compromised.

Another negative aspect is accuracy. With an alphabetical or numeric password, if it is typed correctly, it is one hundred percent accurate. The issue with biometrics is that it is impossible to be perfect. A misread of an iris or a smudge fingerprint can result in a denied login.

The last roadblock concerning biometrics is the price. Implementing a set of biometrics devices can be pricey. The average cost of fingerprint and iris scanners can range from two thousand dollars to ten thousand dollars. A hefty price to pay for any organization given that the technology does have accuracy issues.

K-12 Adoption

Adoption of biometrics in the United States consists mostly of CCTV and other forms of less intrusive biometrics. There are not many implementations of personal data saving biometric systems that are allowed in US schools because of statewide restrictions. The closest analog to seeing how these technologies would work in a K-12 school would be to look at the United Kingdom. The United Kingdom, instead of having FERPA, has the Protections of Freedoms Act of 2012. This act does not prevent the use of biometric technology but requires the school to notify the parents of any student under eighteen that is subject to biometric equipment. The parent could object, and the school is required to stop. This law makes it much easier to adopt biometrics in Europe than it does the United States. A state-of-the-art biometric device that is implemented in K-12 in Europe is the vein reader. The students use the reader to track their attendance when entering the school. The schools then store this data in a database for reference. This data, however, can be deleted if the parent or child wishes to do so in accordance with the

Protections of Freedoms Act of 2012.

Best Practice Model

A particular point of contention (and derivation) is the choice between a default opt-in model or a default opt-out model. In the UK, the best practice model is a default opt-in. The authors of this paper recommend adopting that model in the US. However, that most likely will not be possible given the legal distinctions between those two countries as outlined in this research article.

The best practice for implementing biometrics in US schools would be acquiring parental consent. This is virtually impossible as there would be some parents who would refuse. If the US could find a way to implement rules like the UK, the US could use biometrics by default and if the parent did not want their child in the database they could refuse. A slow implementation of biometric devices and an opt-in model would benefit most schools. The added security for the child coupled with safe data storage practices would be excellent incentives for most parties. If statewide restrictions were overridden, there would be room to gradually add in biometric devices. A slow and gradual adoption of devices, until fully implemented, would be one of the best strategies to implement biometrics.

Conclusions

Biometrics are an effective way to provide security. It is both personal and safe, but with it being so personal, it can run the risk of a privacy breach. With biometrics keeping personal data, such as fingerprints, iris scans and face scans, schools face many challenges implementing this technology. FERPA and other privacy acts in the US prevent these possible privacy breaches. With parental permission, biometric technologies could be incorporated into schools. However, it is a difficult task to get enough parents to consent to that for their children. Statewide laws also prevent implementation of biometrics in some jurisdictions due to privacy issues. Many schools in the UK implemented biometrics by a default opt-in policy and having parents actively opt-out their child's biometric information if they do not agree. Overall, biometrics provide a great amount of personal security but have several issues with technology adoption, especially with minors.

References

Adler, A. (2003). Sample images can be independently restored from face recognition templates. CCECE (pp. 1163-1166). IEEE.

Andreas, S. (2000). The Wall Around the West: State Borders and Immigration Controls in North America and Europe. Boston: Rowman and Littlefield.

Bigo, D. (2002). Security and Immigration: Towards a Critique of the Governmentality Unease. Alternatives, 63-92.

Cappelli, R., Maio, D., Lumini, A., & Maltoni, D. (2007). Fingerprint image reconstruction from Standard Templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(9), 1489-1503.

Ceyhan, A. (2008). Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. Surveillance & Society, 5(2), 102-123.

Frank, R., & Wagner, L. (2018). Understanding the Importance of FERPA & Data Protection in Higher Education. Retrieved November 11, 2020, from

https://digitalcommons.lasalle.edu/cgi/viewcontent.cgi?article=1037&context=mathcompcapstones

Javier Galbally, A. R.-B.-G. (2013). Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. Computer Vision and Image Understanding, 117(10), 1512-1525.

Kowtko. (2014). Biometric Authentication for Older Adults. IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014 (pp. 1-6). Farmingdale, NY: IEEE. doi:10.1109/LISAT.2014.6845213

Leaton Gray S. (2018) Biometrics in Schools. In: Deakin J., Taylor E., Kupchik A. (eds) The Palgrave International Handbook of School Discipline, Surveillance, and Social Control. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-71559-9_21

Marta Gomez-Barrero, C. R. (2014). Protected Facial Biometric Templates Based on Local Gabor Patterns and Adaptive Bloom Filters. 2014 22nd International Conference on Pattern Recognition (pp. 4483-4488). Stockholm, Sweden: IEEE.

Marta Gomez-Barrero, J. G.-G. (2014). A novel hand reconstruction approach and its application to vulnerability assessment. Information Sciences, 268, 103-121.

Mayhew, S. (2015, December 14). UK school using biometric technology to verify students identity and register attendance. Retrieved December 11, 2020, from https://www.biometricupdate.com/201512/uk-school-using-biometric-technology-to-verify-students-identity-and-register-attendance

Senate Bill 855. (2013) Education, 2013 Reg. Sess. (MD. 2013).

Biometric Institute. (2018, December 14). Types of Biometrics. Retrieved November 05, 2020, from https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

Wencheng Yang, J., Yang, J., Wang, S., & Shu, L. (2013). Biometrics for Securing Mobile Payments: Benefits, Challenges and Solutions. Retrieved December 10, 2020, from https://www.researchgate.net/profile/Song_Wang10/publication/269239385_Biometrics_for_securing_mobile_payments_Benefits_challenges_and_solutions/links/556bad5d08aefcb861d61190.pdf