West Coast Publishing

Ban Biometric Recognition File 2 Public Forum April 2023

Research assistance by Kinny Torre

Thanks for using our Policy, LD, and Public Forum evidence and Breaking Down Barriers Instructional Materials.

Please don't share this material with anyone outside of your school

including via print, email, dropbox, google drive, the web, etc.
We're a small non-profit; please help us continue to provide our products.

Contact us at jim@wcdebate.com

www.wcdebate.com

WEST COAST DEBATE

Public Forum

Finding Arguments in this File

Use the table of contents on the next pages to find the evidence you need or the navigation bar on the left. We have tried to make the table of contents as easy to use as possible.

Using the arguments in this File

We encourage you to be familiar with the evidence you use. Highlight (underline) the key lines you will use in the evidence. Cut evidence from our files, incorporate your and others' research and make new files. File the evidence so that you can easily retrieve it when you need it in debate rounds. Practice reading the evidence out-loud; Practice applying the arguments to your opponents' positions; Practice defending your evidence in rebuttal speeches.

Use West Coast Evidence as a Beginning

We hope you enjoy our evidence files and find them useful. In saying this, we want to make a strong statement that we make when we coach and that we believe is vitally important to your success: DO NOT USE THIS EVIDENCE AS A SUBSTITUTE FOR YOUR OWN RESEARCH. Instead, let it serve as a beginning. Let it inform you of important arguments, of how to tag and organize your arguments, and to offer citations for further research. Don't stagnate in these files--build upon them by doing your own research for updates, new strategies, and arguments that specifically apply to your opponents. In doing so, you'll use our evidence to become a better debater.

Copying West Coast Evidence

Our policy gives you the freedom to use our evidence for educational purposes without violating our hard work.

- You may print and copy this evidence for those on your team.
- You may not electronically share nor distribute this evidence with anyone other than those on your team unless you very substantially change each page of material that you share.

For unusual situations, you can e-mail us at jim@wcdebate.com and seek our consent.

Ordering West Coast Materials

1. Visit the West Coast Web Page at www.wcdebate.com
2. E-mail us at jim@wcdebate.com
3. Fax us at 877-781-5058

Visit our web page!

www.wcdebate.com

Table of Contents

WEST COAST DEBATE **2**

Table of Contents **3**

Resolved: The United States Federal Government should ban the collection of personal data through biometric recognition technology. **4**

PRO **5**

Democracy 6

Racist Policing 9

Education 12

Rebuttals **15**

AT: Health 16

AT: Education 17

CON **18**

Contentions **19**

Education 20

Health 22

Counter-Terrorism 24

Gun Violence 25

Crime 27

Rebuttals **29**

AT: Education 30

AT: Democracy 31

Resolved: The United States Federal Government should ban the collection of personal data through biometric recognition technology.

PRO

Democracy

Facial recognition commodifies private data without consent leaving young people particularly vulnerable to unauthorized use of their personal information

Shobita Parthasarathy et al., Professor of Public Policy and Women's Studies, and Director of the Science, Technology, and Public Policy Program, at the University of Michigan, 2020,

"Cameras in the Classroom: Facial Recognition Technology in Schools," (accessed: 03/18/23)

FR in schools is likely to generate new data on students and create new markets in commodifying student data. Previous experience with similar data-generating technologies suggests that providers of these technologies will seek to commodify data collected, creating concerns about ownership, consent, value, and market exploitation. Providers may even offer FR services at no cost in exchange for the ability to collect and monetize the data. There is limited legal and policy clarity about whether citizens own their data. Most cases suggest that though citizens do not have ownership over their biometric data, they have a right to full, informed consent. This framing has been reinforced by the dozens of biobanks that scientists and governments have created over the last few decades, which assert ownership over human DNA samples and other specimens, along with their resulting data. However, given the design of FR tools, which are meant to be applied broadly to any and all faces that move through or near a given system, advance consent may be difficultimpossible to obtain. Further, there is concern that making biometric data collection a routine part of school life, especially without any explicit discussion about where and how to release this data, teaches students that it is normal and unremarkable to give away biometric data and have it used to track your location, purchases, and activities. Altogether, our analysis indicates that the institution of FR in schools threatens students' data privacy and security, will result in data collection without consent, and will create a culture of permissiveness regarding data collection, leaving young people particularly vulnerable to unauthorized use of their personal information.

Facial recognition is inaccurate and threatens the civil and human rights of communities of color as well as queer individuals

Vasudha Talla et al., Immigrants' Rights Program Director of ACLU Northern California, October 19, **2020**,

"Re: Freedom of Information Act request regarding use of Clearview AI Facial Recognition Software," (accessed: 03/18/23)

Facial recognition technology affords government and private actors the unprecedented ability to identify, locate, and track individuals, raising serious civil and human rights and civil liberties concerns. Foremost among those concerns is the impact of the technology on Black people and other over-policed communities, drawing them further into criminal and immigration systems. Facial recognition has been repeatedly demonstrated to be less accurate when used to identify Black people, people of Asian descent, and women.3 Last December, the National Institute of Standards and Technology released results for a comprehensive study of facial recognition systems finding that African American and Asian people were up to 100 more times likely to be misidentified than white men, depending on the algorithm and use case.4 These findings built on an earlier ACLU study, in which 1 in 5 California legislators were erroneously matched to a mugshot of persons who have been arrested, with facial recognition disproportionately misidentifying lawmakers of color.5 Many face recognition algorithms also misgender transgender and gender nonconforming people, while others purport to identify a person's sexual orientation by relying on and perpetuating harmful stereotypes about physical appearance.6 These inaccuracies have led to wrongful detentions for crimes people did not commit, such as the false arrest of Robert Julian-Borchak Williams recently documented in the New York Times.7

Even when accurate, biometric recognition poses an unprecedented threat to individuals' privacy and security

Vasudha Talla et al., Immigrants' Rights Program Director of ACLU Northern California, October 19, **2020**,

"Re: Freedom of Information Act request regarding use of Clearview AI Facial Recognition Software," (accessed: 03/18/23)

Even when the technology accurately identifies people, it poses an unprecedented threat to individuals' privacy and security. Over the past several years, face recognition systems have been used to criminalize poverty, facilitate mass arrests and incarceration of ethnic and racial groups, surveil demonstrators exercising their First Amendment rights at protests, and target immigrants for deportation.8 Last year, the New York Times reported that ICE officials had mined state driver's license databases using facial recognition technology, analyzing millions of driver photos without their knowledge.9 Clearview AI is a software company that has significantly expanded the reach of facial recognition by scraping and scanning billions of personal photos from the internet, including social media sites, to create a massive database. Clearview AI sells access to this trove of information to both law enforcement agencies and private businesses. It has provided accounts to a range of international entities and police departments, including those in countries with explicit anti-LGBTQ laws.10 This development of a massive facial recognition database makes it possible to find people's names and social media accounts or identify them as they protest, shop, and seek essential and sensitive government services.

Corporations are lobbying for weak regulations to protect their profits over the lives of people of color; now is key to time to act for equity and justice

Ashely DelVillar and Myaisha Hayes, Villar is the Digital Privacy Campaign Coordinator at La Resistencia and Hayes is the Campaign Strategies Director at Media Justice, July 22, **2021**,

"How Face Recognition Fuels Racist Systems of Policing and Immigration — And Why Congress Must Act Now" https://www.aclu.org/news/privacy-technology/how-face-recognition-fuels-racist-systems-of-policing-and-immigration-and-why-congress-must-act-now (accessed: 03/18/23)

Big Tech companies like Microsoft are already lobbying for weak regulations that protect their corporate interests and effectively greenlight these dangerous systems. In addition to stopping government acquisition, use, and funding of face recognition technology for state and local face surveillance, the federal government must support local grassroots-powered progress by rejecting Big Tech efforts to preempt state and local bans and moratoria. We can't let Big Tech stamp out our hard-won advancements. We are at a critical moment. The fight against face recognition comes alongside a nationwide reckoning with racism and policing led by the Black Lives Matter movement. We must take this opportunity to recognize the role of surveillance in exacerbating the inherent racism of our law and immigration enforcement systems. We must stop face and other biometric surveillance and confront these systemic harms. Only then will we be on the path to equity and justice.

Face recognition technology threaten privacy, free speech, and black and brown people

Ashely Del Villar and Myaisha Hayes, Villar is the Digital Privacy Campaign Coordinator at La Resistencia and Hayes is the Campaign Strategies Director at Media Justice, July 22, **2021**,

"How Face Recognition Fuels Racist Systems of Policing and Immigration — And Why Congress Must Act Now" https://www.aclu.org/news/privacy-technology/how-face-recognition-fuels-racist-systems-of-policing-and-immigration-and-why-congress-must-act-now (accessed: 03/18/23)

Face recognition technology may sound futuristic, or perhaps too abstract to seem harmful. But we are already living in a reality in which face recognition and other forms of biometric surveillance pervade our daily lives. These technologies threaten our privacy and free speech rights and, when used by police and immigration enforcement, serve as yet another dangerous system to abuse Black and Brown people on a massive scale. Big Tech companies are profiting off these abuses because they are the ones developing and selling face recognition to government agencies. And it's our communities — particularly communities of color — that face the harmful consequences.

Racist Policing

Face recognition technology's proven track record of inaccuracy amplifies racist policing

Ashely Del Villar and Myaisha Hayes, Villar is the Digital Privacy Campaign Coordinator at La Resistencia and Hayes is the Campaign Strategies Director at Media Justice, July 22, **2021**,

"How Face Recognition Fuels Racist Systems of Policing and Immigration — And Why Congress Must Act Now" https://www.aclu.org/news/privacy-technology/how-face-recognition-fuels-racist-systems-of-policing-and-immigration-and-why-congress-must-act-now (accessed: 03/18/23)

Our law and immigration enforcement systems are rooted in this country's racist history, including slavery, and were created to uphold white supremacy. This is why it's often those who sit at the margins — folks of color, immigrants, the poor, disabled, women, and trans or gender nonconforming people — who face systemic violence and brutality. Face recognition technology, which was created by those with the most power in society, will only exacerbate this legacy and pattern of state-sanctioned violence against our communities. We're already seeing this dynamic at work. In Detroit, police use of face recognition led to the wrongful arrest of Robert Williams, a Black man who was arrested at his home in front of his family. Face recognition's proven track record of inaccuracy when used against people of color makes us even more likely to be targeted, arrested, or detained. But even if this technology was perfectly accurate, it would still harm communities of color by facilitating systems that are already racist.

Biometric recognition technology further empowers racial bias and anti-activist surveillance within law enforcement

Alex Najibi, Najibi is a 5th-year Ph.D. candidate studying bioengineering at Harvard University's School of Engineering and Applied Sciences, October 24, **2020**,

"Racial Discrimination in Face Recognition Technology" https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ (accessed: 03/18/23)

Police use face recognition to compare suspects' photos to mugshots and driver's license images; it is estimated that almost half of American adults – over 117 million people, as of 2016 – have photos within a facial recognition network used by law enforcement. This participation occurs without consent, or even awareness, and is bolstered by a lack of legislative oversight. More disturbingly, however, the current implementation of these technologies involves significant racial bias, particularly against Black Americans. Even if accurate, face recognition empowers a law enforcement system with a long history of racist and anti-activist surveillance and can widen pre-existing inequalities.

Biometric recognition stems from an incentivizes racist policing

Alex Najibi, Najibi is a 5th-year Ph.D. candidate studying bioengineering at Harvard University's School of Engineering and Applied Sciences, October 24, **2020**,

"Racial Discrimination in Face Recognition Technology" https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ (accessed: 03/18/23)

Another key source of racial discrimination in face recognition lies in its utilization. In 18th century New York, "lantern laws" required enslaved people to carry lanterns after dark to be publicly visible. Advocates fear that even if face recognition algorithms are made equitable, the technologies could be applied with the same spirit, disproportionately harming the Black community in line with existing racist patterns of law enforcement. Additionally, face recognition can potentially target other marginalized populations, such as undocumented immigrants by ICE, or Muslim citizens by the NYPD. Discriminatory law enforcement practices were highlighted following the murder of George Floyd by the Minneapolis PD. Black Americans are more likely to be arrested and incarcerated for minor crimes than White Americans. Consequently, Black people are overrepresented in mugshot data, which face recognition uses to make predictions. The Black presence in such systems creates a feed-forward loop whereby racist policing strategies lead to disproportionate arrests of Black people, who are then subject to future surveillance. For example, the NYPD maintains a database of 42,000 "gang affiliates" – 99% Black and Latinx – with no requirements to prove suspected gang affiliation. In fact, certain police departments use gang member identification as a productivity measure, incentivizing false reports. For participants, inclusion in these monitoring databases can lead to harsher sentencing and higher bails– or denial of bail altogether.

Biometric recognition is inaccurate with underrepresented groups

The AJL, Algorithmic Justice League is an organization that combines art and research to illuminate the social implications and harms of artificial intelligence, no date

"THE ALGORITHMIC JUSTICE LEAGUE FACIAL RECOGNITION TECHNOLOGY," https://www.ajl.org/facial-recognition-technology (accessed: 03/18/23)

These systems perform with higher inaccuracy rates on underrepresented groups like youth, elderly, women and people with darker skin. This increases the risk that people from these groups will be misidentified as a criminal suspects. Misidentification can lead to serious consequences for a person's liberty and livelihood, particularly if someone is forced to go through the criminal justice system and prove their innocence. Even when misidentified suspects are released, they may lose their jobs and still face death threats and online abuse if the arrest becomes known. In addition to being inaccurate (biased) these technologies are discriminatory because they disproportionately impact certain groups.

Despite its inaccuracies, biometric recognition will become entrenched in institutions

Shobita Parthasarathy et al., Professor of Public Policy and Women's Studies, and Director of the Science, Technology, and Public Policy Program, at the University of Michigan, 2020,

"Cameras in the Classroom: Facial Recognition Technology in Schools," (accessed: 03/18/23)

Further, the cases of CCTV and airport security illuminate how excitement over a technological fix can lead to entrenchment, even if the tool is not necessarily accurate. Just as CCTV rarely deters crime in the UK despite being widely implemented, it is likely that FR, which is similar to CCTV in form and function, could similarly become entrenched despite inaccuracies. These cases also show the sustained resources and training needed to maintain accuracy, the difficulty of assessing accuracy for low-probability events, the problems with having courts as the ultimate arbiters of accuracy, the racial bias that is embedded in surveillance technologies, and the challenge of having local officials determine accuracy among heterogeneous products. Overall, it is difficult to imagine how FR systems will establish and maintain a high level of accuracy in schools.

Education

Biometrics in schools magnifies the school to prison pipeline

Rebecca Heilweil, Reporter, December 20, **2019**,

"Schools are using facial recognition to try to stop shootings. Here's why they should think twice." https://www.vox.com/recode/2019/12/20/21028124/schools-facial-recognition-mass-shootings (accessed: 03/18/23)

Facial recognition requires creating databases of sensitive and personally-identifiable data — immutable information about our faces — that we may not want schools to possess. For one thing, the Surveillance Technology Oversight Project's Cahn is doubtful school officials are prepared to keep such information secure and protected from hackers. But, like other critics, he's also worried about whether these systems will be used to target undocumented students and students of color. "Many school districts have a history of working hand-in-hand with law enforcement to create the school-to-prison pipeline, so we certainly can't trust that schools will push back against a request from law enforcement," Cahn said. "But even if these schools were to oppose [law enforcement], they simply don't have a legal mechanism to block the government from getting a court order to obtain this data."

Facial recognition normalizes surveillance, expands the surveillance state, and causes negative psychological and social effects for students

Shobita Parthasarathy et al., Professor of Public Policy and Women's Studies, and Director of the Science, Technology, and Public Policy Program, at the University of Michigan, 2020,

"Cameras in the Classroom: Facial Recognition Technology in Schools," (accessed: 03/18/23)

Implementing FR in schools will normalize the experience of being constantly surveilled starting at a young age. Furthermore, once implemented, it will be hard to control how administrators use FR and for what purposes. The analogical case of closedcircuit television (CCTV) reveals how surveillance technologies can undergo mission creep: CCTV systems in secondary schools in the United Kingdom (UK) were FR's similarities to CCTV in terms of form and function, it is likely that FR will also undergo mission creep as administrators expand the usage of the technology outside of what was originally defined. The normalization of surveillance will result in negative psychological and social effects for students. CCTV, as well as the cases of fingerprinting in schools and India's Aadhaar system, make subjects feel powerless as they feel that they are always being watched. This is likely to be replicated with FR in schools. Finally, limited data protections in the face of widespread surveillance puts subjects' privacy at greater risk. This was the case with India's Aadhaar system, where citizens' biometric data has been subject to security breaches, and would also be a significant risk in school FR systems.

Facial recognition technology amplifies, institutionalizes, and weaponizes existing racial biases in schools

Shobita Parthasarathy et al., Professor of Public Policy and Women's Studies, and Director of the Science, Technology, and Public Policy Program, at the University of Michigan, 2020,

"Cameras in the Classroom: Facial Recognition Technology in Schools," (accessed: 03/18/23)

Using FR technology in schools is likely to amplify, institutionalize, and potentially weaponize existing racial biases, resulting in disproportionate surveillance and humiliation of marginalized students. It is likely to mimic the impacts of school resource officers (SROs), stop-and-frisk policies, and airport security. All of these interventions purport to be objective and neutral systems, but in practice they reflect the structural and systemic biases of the societies around them. All of these practices have had racist outcomes due to the users of the systems disproportionately targeting people of color. For example, though predictive policing is supposed to remove the bias of individual officers, in practice its deployment in predominantly Black and brown neighborhoods, its training data, and its algorithms all serve to reproduce bias on a systemic level and disproportionately harm Black and brown people, to such an extent that several cities have recently discontinued its use. These cases have also revealed that technologies that target subjects along racist lines result in negative psychological and social outcomes for these subjects. The use of metal detectors in schools decreases students' sense of safety, for example. Because FR is a similar surveillance technology that has potential to amplify user biases, it is likely that FR systems in schools will disproportionately target students of color, harming them psychologically and socially. Finally, FR algorithms consistently show higher error rates for people of color, with white male subjects consistently enjoying the highest accuracy rates. In sum, students of color are more likely to be targeted by FR surveillance and more likely to be misidentified by FR. multiplying the negative impacts of the tool.

Biometric recognition is inaccurate and causes racial discrimination in schools

The Human Rights Watch, June 21, **2019**,

"Facial Recognition Technology in US Schools Threatens Rights" https://www.hrw.org/news/2019/06/21/facial-recognition-technology-us-schools-threatens-rights (accessed: 03/18/23)

Governments are obligated to protect children's lives and safety, and this is the Lockport district's stated goal. However, facial recognition technology comes with a risk of violating people's rights – a particularly serious risk for both children and adults of color. Several studies have documented that facial recognition software can be less accurate for people of color and women than they are for white men, with one study finding that systems were inaccurate for up to 35 percent of darker-skinned women. Formal studies of the technology's accuracy for children appear to be scant – which at a minimum means more research needs to be done. But the risks are real: using inaccurate facial recognition technology in schools could perpetuate racial discrimination against people who have long faced prejudice and exclusion. For years, civil rights activists fought to establish that people of color have a right to enter or move around in buildings – including schools – precisely as white people do. Yet, with faulty facial recognition technology, children of color could soon find themselves forced to deal with a security guard or be singled out in other ways simply to go to school. The same thing could happen to teachers of color, or families of color who want to see the school play or a basketball game. Imagine a line of excited children and parents – then the potential shunting of up to a third of the Black mothers and grandmothers to one side while the white male family members sail through.

Inaccurate biometric in schools are deadly

Benjamin Joe, Reporter, **October 21**, 2022,

"New York Study of Biometric Tech in Schools Nears Completion" https://www.govtech.com/education/k-12/new-york-study-of-biometric-tech-in-schools-nears-completion (accessed: 03/18/23)

Schulz also noted that the system placed in Lockport was credited with having "gun recognition capacity," but testing showed it identified a broom as a gun. The company that sold the technology to the district has since advised it to ignore the gun warnings, he testified. "Any one of those false warnings, false warnings being that if a student of color that got misidentified, if any of those had gotten through to the Lockport Police Department, the chief of police has said it would be treated as a live-shooter situation and armed police officers would be sent into the school because of a false alarm," Shultz said.

Rebuttals

AT: Health

Biometric accuracy is not universal and are particularly inaccurate for black young females

Alex Najibi, Najibi is a 5th-year Ph.D. candidate studying bioengineering at Harvard University's School of Engineering and Applied Sciences, October 24, **2020**,

"Racial Discrimination in Face Recognition Technology" https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ (accessed: 03/18/23)

Face recognition algorithms boast high classification accuracy (over 90%), but these outcomes are not universal. A growing body of research exposes divergent error rates across demographic groups, with the poorest accuracy consistently found in subjects who are female, Black, and 18-30 years old. In the landmark 2018 "Gender Shades" project, an intersectional approach was applied to appraise three gender classification algorithms, including those developed by IBM and Microsoft. Subjects were grouped into four categories: darker-skinned females, darker-skinned males, lighter-skinned females, and lighter-skinned males. All three algorithms performed the worst on darker-skinned females, with error rates up to 34% higher than for lighter-skinned males (Figure 1). Independent assessment by the National Institute of Standards and Technology (NIST) has confirmed these studies, finding that face recognition technologies across 189 algorithms are least accurate on women of color.

Biometrics are healthcare perpetuate inequities

The PEW Charitable Trusts, Nonpartisan thinktank, November **2020**,

"Health Care Can Learn From Global Use of Biometrics" https://www.pewtrusts.org/en/research-and-analysis/reports/2020/11/health-care-can-learn-from-global-use-of-biometrics (accessed: 03/18/23)

As with any technological solution, health care should always consider pertinent challenges and the gaps they may expose. Unwittingly, biometrics could further perpetuate inequities in health care. Despite recent advances, certain modalities and associated algorithms do not work equitably across populations. There are religious and cultural sensitivities that could prevent an individual from submitting or capturing a facial image. In the ID2020 implementation in Indonesia, facial recognition faced challenges when women wore headscarves in the captured images.108 Health care would also need to find ways to implement solutions and policies that meet the needs of pediatric populations. This could include more frequent collection of images as features and characteristics change with age or allowing parents to provide consent to collect biometrics until the patient reaches a specified age. Further, individuals with dermatological conditions such as eczema cannot provide digital fingerprints that would work in an indexing system. Similarly, those missing digits or those who have degenerative conditions would also require alternative options.109

AT: Education

Biometric recognition technology always expands the surveillance state: there is not a single example of a surveillance tool that does only what it is supposed to do

Rebecca Heilweil, Reporter, December 20, **2019**,

"Schools are using facial recognition to try to stop shootings. Here's why they should think twice." https://www.vox.com/recode/2019/12/20/21028124/schools-facial-recognition-mass-shootings (accessed: 03/18/23)

Facial recognition could do more than notify officials when people suspected to be dangerous enter schools. For school officials, that might seem like more bang for their buck, but critics worry that excessive use of the tool could turn into surveillance of students. "We don't have a single example of a costly and invasive surveillance tool that's deployed that's only used for the thing we're told it will be," Cahn said. Mike Vance, RealNetworks's product management senior director, says that schools are using facial recognition to preemptively enforce child custody agreements. He gave examples of schools that have set alerts in their facial recognition systems on birth parents who have been barred by court order — or other legal processes — to make contact with a child. (He's not aware of any cases in which a school has caught a parent in this way.) Wired reported that a facial recognition system was even used to check whether a student believed to have run away from home had shown up at school.

There is no evidence that biometrics provide any benefits to public safety

Rebecca Heilweil, Reporter, December 20, **2019**,

"Schools are using facial recognition to try to stop shootings. Here's why they should think twice." https://www.vox.com/recode/2019/12/20/21028124/schools-facial-recognition-mass-shootings (accessed: 03/18/23)

High-tech security software could make students feel policed and surveilled, and research has already demonstrated that facial recognition can be inaccurate, especially for people of color and women, as well as other groups. (Those findings were confirmed by a National Institute of Standards and Technology report released Thursday.) Meanwhile, legislation explicitly regulating the use of these tools remains scant, and some critics worry that the sensitive data that facial recognition systems create could ultimately be shared with law enforcement, or a federal agency such as Immigration and Customs Enforcement (ICE). "Facial recognition is biased, broken, and it gets it wrong. It's going to put a lot of students in danger, especially students of color," warns Albert Fox Cahn, the executive director and founder of a legal nonprofit called the Surveillance Technology Oversight Project. "We know that this technology will get it wrong quite a bit, and we also have no evidence to show that it has any public safety benefit whatsoever, especially in the grandiose scenarios that proponents put forward."

CON

Contentions

Education

Biometric data Is crucial to effective education

Marcela Henandez de Menendez et al., Professor at Tecnológico de Monterrey, July 28, **2021**,

"Biometric applications in education" https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8318548/ (accessed: 03/18/23)

Due to their influence on learning, emotional states play a crucial role in education in general. Boredom has been shown to influence learning, while engagement can positively improve learning outcomes. Frustration and confusion can positively affect learning if the student can resolve these states. Estimating prediction in real-time of student's affective states is a research topic of great interest due to its benefits through different intervention strategies [24]. The collection of appropriate biometric data and the analysis of physiological and behavioral patterns during a learning experience can help introduce proper interventions to improve the learning experience as the main hypotheses in this domain. Biometrics provides an objective measure of the physiological reactivity of users that is used to infer affective states. Electrodermal activity, skin temperature, and heart rate showed high performance as predictors of emotions [34, 35, 55]. Wampfler et al. [73] predict a student's affective states (while solving math exercises) using arbitrary writing and drawing assignments (based on stylus data).

Educational institutions are using biometric technology to be more efficient for students and faculty

Marcela Henandez de Menendez et al., Professor at Tecnológico de Monterrey, July 28, **2021**,

"Biometric applications in education" https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8318548/ (accessed: 03/18/23)

Educational institutions are acquiring novel technologies to help make their processes more efficient and services more attractive for both students and faculty. Biometric technology is one such example that has been implemented in educational institutions with excellent results. In addition to identifying students, access control, and personal data management, it has critical applications to improve the academic domain's teaching/learning processes. Identity management system, class attendance, e-evaluation, security, student motivations, and learning analytics are areas in which biometric technology is most heavily employed. A literature review is performed to present an overview of biometric technology applications for educational purposes, challenges that must overcome to implement biometric technology, and potentially foreshadowing trends effectively. The future seems promising for biometric technology; the biometric technology market is expected to reach a value of USD 94 billion by 2025 at a compound annual growth rate of 36%. New characteristics are under development for commercial applications, such as vascular pattern recognition, ear shape recognition, facial thermography, odor sensing, gait recognition, heartbeat authentication, brain waves, and human body bioacoustics. The biggest challenge this technology must overcome is security and privacy issues, which must be addressed to fully develop the technology to its full potential. It is desirable that this literature review can provide researchers with a sound vision of the potential that biometric technology will have in education.

Biometric is key to physical and digital security in education

Marcela Henandez de Menendez et al., Professor at Tecnológico de Monterrey, July 28, **2021**,

"Biometric applications in education" https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8318548/ (accessed: 03/18/23)

Biometrics is a useful technology to identify students and ensure no outsiders either in class or on the university's campus. On the other hand, this technology can be used in combination with surveillance cameras to detect strangers. In addition, a blocking protocol can be activated in an emergency on campus to ensure that no one enters or leaves. Using identification chips (based on radio frequency) and combining them with intelligent data, students can be located to guarantee their safety. Biometric systems can also limit access to computers, emails, websites, and other restricted educational tools (assessments) [29]. Finally, students' presence on campus can be tracked by knowing at any time where they are, when they arrived and left, and where they went [18]. Higher Education is becoming one of the most popular targets for cyberattacks because universities have relatively open networks. For example, universities have several wireless networks that connect their areas using multiple bandwidths; these multiple networks lead to an output that contains student data (payment information, social security number, personal addresses, etc.). Additionally, universities must comply with various laws to protect student data; these law's guidelines may restrict the institution's IT infrastructure or leave it vulnerable to hackers (Bio-KeyTM, n.d.).

Health

We can learn from the world's history with biometrics to provide the best healthcare

The PEW Charitable Trusts, Nonpartisan thinktank, November **2020**,

"Health Care Can Learn From Global Use of Biometrics" https://www.pewtrusts.org/en/research-and-analysis/reports/2020/11/health-care-can-learn-from-global-use-of-biometrics (accessed: 03/18/23)

The use of biometrics in industries around the world provides valuable insight for implementing any solution to resolve one of the most persistent and vexing problems in health care: patient matching. Building on the lessons learned from these applications, patients, the health care industry, and policymakers can weigh concerns against benefits and make informed decisions about the best methods and strategies for integrating biometrics. This technology can help providers and patients have more complete and accurate health information to inform treatment decisions when used as part of a larger solution for patient matching. With collaborative, cross-sector leadership, health care can design a system incorporating biometrics that prioritizes both interoperability and privacy while working to better link records across different sites of care.

Biometric data in healthcare can be protected

The PEW Charitable Trusts, Nonpartisan thinktank, November **2020**,

"Health Care Can Learn From Global Use of Biometrics" https://www.pewtrusts.org/en/research-and-analysis/reports/2020/11/health-care-can-learn-from-global-use-of-biometrics (accessed: 03/18/23)

As the Estonian e-ID example demonstrated, even with protections in place, breaches occur. However, because Estonia had risk mitigation plans and invested users, the country quickly addressed the breach, had open channels of communication with citizens, and pushed out a technical fix to every national e-ID card. Despite this threat, citizens continued using their e-IDs; Estonians' access to digital tools and services through their e-ID became an expected way of life.122 Because health care data is sensitive and already enjoys some protections, users who access this information are regulated and audited. Similar protections could be implemented in a biometric-based system and may already confer from existing policies, such as those implementing HIPAA. In addition, health care already adheres to policies and procedures for HIPAA violations and inappropriate access to data; these same approaches may transfer to biometric data.

Biometrics are key to increase the quality and efficiency of healthcare

The PEW Charitable Trusts, Nonpartisan thinktank, November **2020**,

"Health Care Can Learn From Global Use of Biometrics" https://www.pewtrusts.org/en/research-and-analysis/reports/2020/11/health-care-can-learn-from-global-use-of-biometrics (accessed: 03/18/23)

Yet despite widespread use of biometrics in a range of industries, these tools are not employed in the United States to address a key problem that has plagued the health care system for decades: patient matching, or the ability to accurately link health records for the same person across different sites of care, such as multiple hospitals and clinics. Patients often visit multiple health care providers, and patient records from one facility may have information on diagnoses, lab test results, or other data critical to providers at another institution. Accurate patient matching would help ensure that the doctors, nurses, and other clinicians caring for a patient across a range of health care facilities have the information they need to offer high-quality, coordinated, and safe care. Current patient matching approaches in the U.S. typically rely on simple demographic data such as names, addresses, and/or birthdates. However, match rates when sharing this information among health care facilities can be as low as 50%, with errors resulting from typos, changing data (e.g., when patients move), similar data (e.g., same name and birthdate), and many other factors. Given the limitations of this demographics-based system, the federal government and Congress have examined alternatives, including whether to establish a unique patient identification solution, which could involve biometrics, assigning patients a number, or other solutions.

Counter-Terrorism

Biometrics is used to detect criminals and terrorists as well as to protect critical infrastructure

UN Security Council Counter-Terrorism Committee Executive Directorate, No Date,

"CTED Analytical Brief: Biometrics and Counter-Terrorism" (accessed: 03/18/23)

Biometrics have become more prevalent in efforts to detect criminals, known terrorists, and individuals suspected of terrorist offences, including in public spaces, with facial recognition systems used in conjunction with CCTV video surveillance. Recognition technology has also been coupled with unmanned aircraft systems (UAS) in a law enforcement and border control context, helping to control large crowds and assist in the identification of individuals in public spaces (as identified in CTED's related Trends Alert).6 The use of biometrics in counter-terrorism is often connected to the development and utilization of emerging technologies. This has included techniques to identify individuals of interest – for example high-definition cameras, matching algorithms, and artificial intelligence (AI), sometimes in conjunction with a linked database (e.g., terrorist watchlists) – and the use of biometrics (including multi-biometrics access control systems) to protect critical infrastructure sites and facilities, as well as "soft" targets, from terrorist attacks.7

Biometrics are key to countering the financing of terrorism

UN Security Council Counter-Terrorism Committee Executive Directorate, No Date,

"CTED Analytical Brief: Biometrics and Counter-Terrorism" (accessed: 03/18/23)

As noted in a recent Financial Action Task Force (FATF) report,8 biometric technologies may also be increasingly helpful for countering the financing of terrorism, offering enhancements to know-your-client (KYC) and customer due diligence (CDD) processes and alternatives to financial institutions' monitoring of banking relationships. CTED's dialogue with Member States, conducted on the Committee's behalf, has revealed that, although the extent of biometrics use and expertise varies significantly, 118 of the 193 United Nations Member States have made at least marginal progress in introducing biometrics for counter-terrorism purposes9 (see table 2, below).

Gun Violence

Biometric recognition could stop millions of children from dying of gun violence

Andres Paciuc, JD candidate at Duke, June 05, **2020**,

"Smart Guns: An Effective Solution or a Waste of Resources?"
https://firearmslaw.duke.edu/2020/06/smart-guns-an-effective-solution-or-a-waste-of-resources/
(accessed: 03/18/23)

Generally, there are two main types of personalized smart guns: (1) biometrical based trigger locks and (2) radio frequency identification (RFID) trigger locks. The former consist of fingerprint or palm-based readers that unlock the firearm when the user's biometric information is recognized. This is similar to the technology used to unlock smart phones. The latter use electromagnets and radio waves to unlock a trigger only when the weapon is proximate to an electronically matched external device (such as a chip-enabled token). Once the gun's locking mechanism is deactivated, the gun can be fired. Proponents of smart gun technology have argued that smart guns could help prevent suicides and accidental firearm discharges, especially involving young people. 4.6 million children live in a home with an unlocked and loaded firearm. Thirty five percent of all gun-related deaths of young people (ages 10-19) were suicides in 2016. In 2017, 43% of youth suicides were committed with a firearm. Importantly, more than 80% of children and adolescent firearm suicides involved a firearm belonging to a family member. This statistic, coupled with the vast number of children in the United States who live in a home with an unlocked, loaded firearm, helps explain why firearm suicide among youths occurs at these rates.

Biometric recognition solves accidental gun deaths

Andres Paciuc, JD candidate at Duke, June 05, **2020**,

"Smart Guns: An Effective Solution or a Waste of Resources?"
https://firearmslaw.duke.edu/2020/06/smart-guns-an-effective-solution-or-a-waste-of-resources/
(accessed: 03/18/23)

Accidental gun deaths are another type of preventable tragedy. There have been at least 1,714 unintentional shootings of children since 2015. Unintentional deaths comprised 26% of all firearm deaths among children (ages 1 – 9 years old) in 2016. Additionally, studies suggest that there are strong correlations between the presence of a firearm at home and an increased likelihood of accidental child firearm deaths. The issue has become even more pressing with the recent increase in unintentional shootings by children during the COVID-19 pandemic, which has coincided with an increase in gun sales during quarantine. By only allowing the authorized user to fire the firearm, smart guns have the potential to prevent youth suicide and accidental gun deaths, without preventing an authorized user from accessing a firearm in case of emergency.

Biometrics are key to gun safety

Steven Zeitchik, Reporter, May 27, 2022,

"Could smart guns save lives?" https://www.washingtonpost.com/technology/2022/05/27/smart-guns-fingerprints-uvalde-teen-suicides/ (accessed: 03/18/23)

Smart-gun technology, also known as "personalized guns," could also prevent fatalities in the case of stolen guns in prison and other settings, advocates say. And teen suicide often involves a gun belonging to an adult that has been found by an underage person in the home. Overall, there were 24,292 gun-related suicides in 2020, more even than the 19,384 murders, according to the Centers for Disease Control and Prevention. "The bottom line is that the gun industry should be innovating to make their products safer, not more deadly," said Nick Suplina, senior vice president of law and policy at the gun-control group Everytown for Gun Safety. Smart-gun technology uses biometric data such as fingerprints — and radio-frequency identification (RFID) transmitted by ring or wristband — to unlock a gun for its legal owner. After years of engineering delays and political resistance, smart guns now appear at least to be nearing the market.

Crime

Biometric recognition is used to solve thousands of crimes

Salam Al Amir, Journalist, March 09, 2023,

"How Dubai Police use biometric technology to fight crime" https://www.thenationalnews.com/uae/2023/03/10/how-dubai-police-use-biometric-technology-to-fight-crime/ (accessed: 03/18/23)

While facial recognition and fingerprint technology is used by police around the world, there are other ways to catch criminals. This new age of policing means that those who break the law can still be identified, even if they wore a mask and gloves, and ensured no DNA evidence was left at the scene. If a suspect is disguised or CCTV footage is too grainy, officers can analyse characteristics such as a person's gait and the shape of their hands and ears to build a clearer picture of who they are. Footage can be compared to a comprehensive video database that includes recordings from CCTV cameras. Dubai Police said the advanced technology, which they have used since 2016, helped officers to make more than 3,000 arrests last year. The technology proved particularly useful during the Covid-19 pandemic, when people wore masks outdoors and when visiting indoor venues. "To identify suspects through gait patterns, a biometric system uses specialised cameras such as LiDAR cameras to capture the movement of an individual's body," said Lt Col Dr Hamad Al Awar, head of video and image examination at Dubai Police's forensic e-evidence department.

Violent crime rates are dramatically increasing

Ames Grawet and Noah Kim, Grawert is senior counsel and John L. Neu Justice Counsel in the Brennan Center's Justice Program and Kim is a Research and Program Associate in the Brennan Center's Justice Program, July 12, 2022,

"Myths and Realities: Understanding Recent Trends in Violent Crime" https://www.brennancenter.org/our-work/research-reports/myths-and-realities-understanding-recent-trends-violent-crime?ms=gad_violent%20crime_617000456634_8626214133_143843260761&gclid=Cj0KCQjwwtWgBhDhARIsAEMcxeDriqJSICYkqp-AIeUzHs8NSYgUp-CN8aQXDLGTkFqhGwXlYi_89dAaAq46EALw_wcB (accessed: 03/18/23)

Crime rates changed dramatically across the United States in 2020. Most significantly, the murder rate — that is, the number of murders per 100,000 people — rose sharply, by nearly 30 percent. Assaults increased as well, with the rate of offenses rising by more than 10 percent. Both increases are part of a broader surge in gun violence. More than 75 percent of murders in 2020 were committed with a firearm, reaching a new high point, and cities that report data on shooting incidents, like New York, saw significant increases in this form of violence as well.

Crime rates have increased nationwide and in all jurisdiction types

Ames Grawet and Noah Kim, Grawert is senior counsel and John L. Neu Justice Counsel in the Brennan Center's Justice Program and Kim is a Research and Program Associate in the Brennan Center's Justice Program, July 12, 2022,

"Myths and Realities: Understanding Recent Trends in Violent Crime" https://www.brennancenter.org/our-work/research-reports/myths-and-realities-understanding-recent-trends-violent-crime?ms=gad_violent%20crime_617000456634_8626214133_143843260761&gclid=Cj0KCQjwwtWgBhDhARIsAEMcxeDriqJSICYkqp-AIeUzHs8NSYgUp-CN8aQXDLGTkFqhGwXlYi_89dAaAq46EALw_wcB (accessed: 03/18/23)

Murders rose in cities nationwide and jurisdictions of all types. Relative to 2019, the number of murders jumped by more than 30 percent in the largest cities and by 20 percent in places designated by the FBI as "suburban" — cities with fewer than 50,000 inhabitants that are within a Metropolitan Statistical Area. Murders rose by comparable levels in rural areas too — an important fact that is only now beginning to receive press attention. Despite politicized claims that this rise was the result of criminal justice reform in liberal-leaning jurisdictions, murders rose roughly equally in cities run by Republicans and cities run by Democrats. So-called "red" states actually saw some of the highest murder rates of all. This data makes it difficult to pin recent trends on local policy shifts and reveals the basic inaccuracy of attempts to politicize a problem as complex as crime. Instead, the evidence points to broad national causes driving rising crime.

Rebuttals

AT: Education

Biometrics are critical to improving the teaching and learning processes in education

Marcela Henandez de Menendez et al., Professor at Tecnológico de Monterrey, July 28, **2021**,

"Biometric applications in education" https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8318548/ (accessed: 03/18/23)

There is also another exciting field of biometrics, in which the emotional and cognitive state of people are detected. This can be used to monitor student's behavior/emotions and change the educational process appropriately. For example, researchers argue that boredom negatively influences learning, whereas engagement improves learning outcomes; biometric sensors have been used to measure electrodermal activity, skin temperature, and heart rate, all good predictors of emotions [73]. Biometrics allows academic institutions to save time, money and also improve educational and non-educational activities. They also offer convenience, safety, and security. Various applications are identified: school access, control of attendance, food service, access to library and media center, bus transportation, control staff time, among others (Fry and Dunphy, n.d.). In addition to identifying students, access control, and personal data management, it has critical applications to improve teaching/learning processes in the educational domain, Fig. 3.

Biometric technology can stop school shootings and gun violence in general

Sam Levin, Correspondent for the Guardian US, February 24, **2016**,

"Smart guns: could fingerprint technology solve America's shooting deaths?" https://www.theguardian.com/technology/2016/feb/24/personalized-smart-guns-biometric-access-fingerprints-gun-control (accessed: 03/18/23)

But in a country that has repeatedly failed to pass meaningful laws restricting access to firearms – even after the unimaginable tragedy of a mass shooter killing 20 young schoolchildren – technological innovation is a critical area in which the US can make progress on preventing gun deaths, participants at the symposium said. "Legislation isn't going to happen," said Ralph Fascitelli, president of Washington CeaseFire. "We can do this. Just give us a chance … We can save thousands of lives." Smart guns could help prevent suicides, accidental shootings, street violence and mass shootings, advocates argue. Two million children, for example, live in a home with a firearm that is loaded and unlocked, and children accidentally shot at least 265 people in 2015.

AT: Democracy

Biometrics are key to preventing fraud and the manipulation of democractic institutions

Hannah Quay-de la Vallee, Vallee is a Senior Technologist at the Center for Democracy & Technology with a PhD in computer science from Brown University, June 07, 2022,

"Public Agencies' Use of Biometrics to Prevent Fraud and Abuse: Risks and Alternatives" https://cdt.org/insights/public-agencies-use-of-biometrics-to-prevent-fraud-and-abuse-risks-and-alternatives/ (Accessed: 03/18/23)

To address these dual issues of fraud and inefficiency (or waste), many agencies turned to biometric-based systems, both to help more effectively identify fraudulent actors to avoid paying out erroneous benefits or avoid providing services to ineligible individuals and more quickly verify legitimate applicants to distribute benefits in an efficient way. As technology is allowing more digital interactions between people and the government, the question of identity verification has become more complex, as agencies can no longer rely on in-person verification with a government ID, nor is it always feasible for beneficiaries. As a result, public agencies are increasingly turning to data sharing and technology to make service delivery easier and more efficient while limiting fraud and waste.

Biometrics provide a means to secure elections without draconian measures that hurt minorities

James Angel, Ph.D and an associate finance professor at Georgetown University's McDonough School of Business, February 20, **2017**,

"A simple, just fix to voter fraud: Take fingerprints" https://thehill.com/blogs/pundits-blog/presidential-campaign/320343-a-simple-just-fix-to-voter-fraud-take-fingerprints/ (accessed: 03/18/23)

Political parties that propose draconian measures are hurting their chances with minority voters, who see voter ID laws as nothing more than thinly veiled attempts to resurrect Jim Crow. Fortunately, there is an easy way to deter voter fraud and provide strong evidence with which to convict fraudsters — fingerprints. If a person shows up at the polls without proper identification, they should be required to leave a fingerprint. They could put a fingerprint on a form on which they attest their identity under penalty of perjury. This process would be very cheap. It costs next to nothing to take a fingerprint, and follow up investigations would only be needed if there were other suspicions of voter fraud or the election was close enough to require a recount. Everyone has fingerprints, so there is no possibility of someone showing up without identification.