BANNING BIOMETRIC DATA COLLECTION WILL BE EFFECTIVE (PRO)	7
EFFECTIVENESS (& DEFINITIONS)	7
DEF: Biometric DataCUSO Magazine, January 30, 2023	<b>7</b>
PRO: Alternative Information Still Available (ex. Photos, ID Cards, etc.)	7
PRO: Regulations are Ineffective	7
PRO: Lack of Accountability for Abuses	
PRO: Lack of Transparency Prevents Enforcement (Ban = Clear Policy)  Civil Liberties Union for Europe, October 25, 2022	<b>7</b> 7
PRO: Regulations are Ineffective (ex. Rules are Vague / Lack Transparency)  Civil Liberties Union for Europe, October 25, 2022	<b>8</b>
PRO: Biometric Data Collection Impacts Millions	
SECURITY CONCERNS	9
PRO: Avoiding Data Breaches/Vulnerabilities Tech Research Online, September 2, 2021	<b>9</b>
PRO: Data breaches CEO World Magazine, May 9, 2022	
PRO: not always accurate	
PRO: Deepfakes Fool AlCX Today, June 3, 2021	
PRO: Police Still Have Sufficient Access Tech Research Online, September 2, 2021	
PRO: Data Breaches from Collecting Data (ex. 50m Users of Facebook!) BBN Times, November 02, 2022	<b>9</b>
PRO: Risks from Outside Applications (ex. Smart Phones) Harvard Business Review, December 6, 2017	<b>10</b>
PRO: Misuse of Data Collection	
PRO: Data Breech Impacts School Children (ex. New York)  The Conversation, November 29, 2022	
PRO: Biometric Technology Can Be Manipulated	<b>10</b>
PRO: Harm to Childrens' Security is 'Very Real' The Conversation, November 29, 2022	
PRO: Biometric Errors Punish Innocent PeopleFoundation for the Future, January 26, 2022	
PRO: Theft of Biometric Data is Permanent	11

SECURITY CONCERNS (CONTINUED)	9
PRO: Security Vulnerabilities from Information Being Hacked  Civil Liberties Union for Europe, October 25, 2022	<b>11</b>
PRO: Facial Recognition Data Vulnerable to Breaches	<b>11</b>
PRIVACY CONCERNS	12
PRO: Users' privacyCEO World Magazine, May 9, 2022	
PRO: Extremely Sensitive Privacy IssuesCX Today, June 3, 2021	
PRO: Privacy Loss a Significant Downside	
PRO: Surveillance State Threatens Freedom	
PRO: Government Data for Tracking and Profiling	<b>12</b>
PRO: Violating Workers' Rights and Privacy Industry Today, February 21, 2023	
PRO: Scanning 97% of Airline Passengers (It's Mass Surveillance)	
PRO: Harm to Childrens' Privacy is 'Very Real' The Conversation, November 29, 2022	
PRO: Tracking People Without Them Realizing	
PRO: Serious Consequences to Privacy Stanford University's Cyber Policy Center, Stanford University, April 23, 2020	
PRO: Facial Recognition Violates Privacy Foundation for the Future, January 26, 2022	
PRO: Infringement on individual privacy	
PRO: Facial Recognition Collects Without Consent	<b>14</b>
VIOLATING CIVIL AND HUMAN RIGHTS	15
PRO: Facial Recognition "Chills" Freedom (& Rights) Foundation for the Future, January 26, 2022	
PRO: Infringement on Freedom of Speech from Mass Surveillance	
PRO: Violating Presumption of Innocence	
PRO: Infringing on 1st Amendment Freedoms (ex. Chills Speech/Assembly)	
PRO: Using Facial Recognition Data is Intrusive	
PRO: Using Facial Recognition Data Threatens Freedoms (ex. Intimidation)	<b>15</b>

DISCRIMINATION/RACISM CONCERNS	16
PRO: Risks of Discrimination and Racial Bias	
PRO: Increased Risk of False Allegations (Due to Misidentification)	<b>16</b>
PRO: Misidentification and Racial BiasStanford University's Cyber Policy Center, Stanford University, April 23, 2020	
PRO: Racial Bias in Data Causes Misidentification	<b>16</b>
PRO: Misidentification Leads to Discrimination & False Arrest	
PRO: Discrimination Against "People of Color"	
PRO: Facial Recognition Technology Threatens Minorities  Civil Liberties Union for Europe, August 3, 2021	
BUSINESSES EXPLOIT WORKERS & CUSTOMERS	17
PRO: Companies Collecting Data for Exploiting Customers	
PRO: Tracking People Without Them Realizing	
COST AND ECONOMIC CONCERNS	18
PRO: Tremendous CostsCEO World Magazine, May 9, 2022	
PRO: Increased Storage Requirements (& Costs)	<b>18</b>
PRO: Failure to Delete Biometric Data (ex. Texas vs. Google)  CUSO Magazine, January 30, 2023	
PRO: Facial Recognition is Expensive (ex. Businesses Suffer) Foundation for the Future, January 26, 2022	
PRO: Facial Recognition Wastes Taxes & Causes Inflation  Foundation for the Future, January 26, 2022	

BANNING BIOMETRIC DATA COLLECTION WILL NOT BE EFFECTIVE (CON)	19
EFFECTIVENESS (EX. NO NEED, BAN = INEFFECTIVE, & REGULATIONS = PREFERABLE)	19
CON: Current Laws and Lawsuits Prevent Abuse (No Need for Ban!)	<b>19</b> 19
CON: Many States Considering/Pursuing Regulations CUSO Magazine, January 30, 2023	<b>19</b>
CON: Regulations are Key (ex. Banning is too Extreme!)	<b>19</b>
CON: Increased Regulation for Biometric Data Collection	<b>19</b>
CON: Lawsuits Hold Companies/Governments Accountable Epiq Global, Last Accessed: April 2023	<b>19</b>
CON: Data Not Intended for Malicious Purposes (ex. Security is the goal)	<b>20</b>
CON: Abandoning New Technologies is Ridiculous (No Malicious Intent!)	
CON: Increased Efficiency and Accuracy	
CON: Punishment Prevents Abuse (ex. Facebook & Clearview Al)	
SECURITY CONCERNS	21
CON: High-security assuranceCEO World Magazine, May 9, 2022	
CON: Difficult to fake	
CON: Deepfakes Extremely DifficultCX Today, June 3, 2021	
CON: Improving Safety in Public Spaces (ex. Banks, Airports) Tech Research Online, September 2, 2021	21
CON: Preventing Illegal Activities (ex. Airport and Border Security)  Tech Research Online, September 2, 2021	
CON: Enhanced Financial Security (ex. Preventing Bank Fraud) Tech Research Online, September 2, 2021	
CON: Biometrics Necessary to Catch Criminals	
CON: Liveness Detection & Protection Tech Research Online, September 2, 2021	
CON: 3D Depth-Sensing Protections Tech Research Online, September 2, 2021	22
CON: Deepfake Detection & Protection Tech Research Online, September 2, 2021	22
CON: Deterring Criminals (ex. ID Theft)	

SECURITY CONCERNS (CONTINUED)	21
CON: Numerous Security Protections	
CON: Unparalleled Effectiveness	22
CON: Avoiding Errors in Identifying Criminals/Terrorists	23
CON: Hack Proof ID (ex. Experts Failed vs Apple iPhone)	23
CON: Biometrics Provide Enhanced Security	23
CON: Biometrics Produce High Accuracy	23
CON: Reducing Fraud-Based CrimesCUSO Magazine, January 30, 2023	23
CON: Higher Security for Less CostCUSO Magazine, January 30, 2023	24
CON: Identifying Serious Threats Quickly	24
CON: Making Schools SaferStanford University, April 23, 2020	
CON: Facial Recognition Identifies Criminals (via CCTV)	24
CON: Facial Recognition Significantly Improves Security  Foundation for the Future, January 26, 2022	24
CON: Facial Recognition Improves Personal Security Foundation for the Future, January 26, 2022	24
CON: Facial Recognition Reduces Security RisksFoundation for the Future, January 26, 2022	<b>24</b> 24
CON: Increased Reliability in Personal Security (ex. No Passwords)	
CON: Biometrics Can Improve Security	
HURTING BUSINESSES	26
CON: Increased Quality of Customer Experience	
CON: Excellent Candidate for AutomationCX Today, June 3, 2021	
CON: Automation Reduces Chance of Errors  BBN Times, November 02, 2022	26
CON: Biometric Data Improves Workplace ProductivityIndustry Today, February 21, 2023	26
CON: Improved Workplace Security	

HURTING BUSINESSES (CONTINUED)	26
CON: Preventing Theft and Fraud	
UNDERMINES RESCUE EFFORTS (EX. HUMAN TRAFFICKERS)	27
CON: Rescuing Children from Human Traffickers	
CON: Helpful for Identifying Lost Children	
CON: Facial Recognition Locates Missing Persons	<b>27</b>
LOSS OF CONVENIENCE	27
CON: Convenience - Easy to useCEO World Magazine, May 9, 2022	
CON: Easy to integrate	
CON: Facial Recognition Improves Efficiency Foundation for the Future, January 26, 2022	
UNDERMINING HELP FOR VULNERABLE GROUPS (EX. HEALTH, HOMELESS, &	& WELFARE) 28
CON: Undermining Health Treatments Tech Research Online, September 2, 2021	<b>28</b>
CON: Identifying Patients and Diagnosis Stanford University's Cyber Policy Center, Stanford University, April 23, 2020	
CON: Protecting Vulnerable Groups (ex. Homeless, Welfare, Etc.)	
CON: Facial Recognition Reduces Spread of DiseaseFoundation for the Future, January 26, 2022	
CON: Biometrics Increase Efficiency	<b>28</b>
BIBI IOGRAPHY	29

# **BANNING BIOMETRIC DATA COLLECTION WILL BE EFFECTIVE (PRO)**

## **Effectiveness (& Definitions)**

**DEF: Biometric Data** 

CUSO Magazine, January 30, 2023

https://cusomag.com/2023/01/30/the-risks-and-rewards-of-biometric-data/

Although there is no exact consensus on the definition of the biometric data that must be protected, the trigger for review is any data that measures a person's unique physical characteristics, including but not limited to fingerprints, palmprints, voiceprints, facial, retinal, or iris measurements, that can be used to identify a unique individual.

## PRO: Alternative Information Still Available (ex. Photos, ID Cards, etc.)

CUSO Magazine, January 30, 2023

https://cusomag.com/2023/01/30/the-risks-and-rewards-of-biometric-data/

Exclusions include examples such as writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, and physical descriptions such as height, weight, hair color, or eye color. Therefore, capturing a driver's license would not be considered "biometric" although the license would still need to be transmitted and stored securely due to other laws protecting consumer information.

#### PRO: Regulations are Ineffective

Harvard Business Review, December 6, 2017

https://hbr.org/2017/12/biometrics-wont-solve-our-data-security-crisis

Unfortunately, it would be naïve to believe that a self-regulating approach to these types of data collection behaviors will work. The information to be gained from a marketer's perspective is just too juicy. The only way to ensure that businesses and government, as well as the public they serve, can move to the next stage in identification and security is to legislate restrictive uses of these types of authentication data and the information gleaned from it. While general consensus under privacy regimes in North America and Europe is that biometric data is personal information, the restrictive use of that data under both current and pending regulations is opaque at best.

## PRO: Lack of Accountability for Abuses

Stanford University's Cyber Policy Center, Stanford University, April 23, 2020

https://hai.stanford.edu/news/challenges-facial-recognition-technologies

Questions also arise around proper oversight of the people creating and implementing the technology. If a police force's outdated facial recognition software produces bad results, who's responsible? Should private companies be held accountable if their technologies are used for nefarious ends?

### PRO: Lack of Transparency Prevents Enforcement (Ban = Clear Policy)

Civil Liberties Union for Europe, October 25, 2022

https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518

Transparency is important because it allows for better control of how your data is processed: you can make sure that companies, for instance, follow the law and respect your individual rights by verifying that information obligations are respected, or verifying that you can access your personal data. If it is not the case, you can then file a complaint with the authority control. Without transparency, companies can do what they want with your personal data without your knowledge, and people do not know who possesses their biometric data and for what purpose. People could be subjected to targeted ads, profiling etc. or their data could be sold to a third-party entity. As an example, the above mentioned Clearview Al harvested pictures of people on the internet without their consent and used it to build their database, which was then used by private companies. After two years of legal dispute, Clearview Al reached an agreement with the American Civil Liberties Union to permanently halt the sales of its biometric database to private companies and individuals in the United States.

# Effectiveness (Continued...)

PRO: Regulations are Ineffective (ex. Rules are Vague / Lack Transparency)

Civil Liberties Union for Europe, October 25, 2022

https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518

Transparency regarding data collection, management and deletion is still too low in practice in the EU; sanctions are often pronounced against companies or institutions for insufficient fulfillment of information obligations. The GDPR requires concise, transparent, comprehensible and easily accessible information to data subjects (Art. 12, 13, 14). For instance, in many cases concerning the use of facial recognition, it is impossible to identify data collectors and processors because you might not know you are being recorded. And even if they are identified, the amount of data collected and the purpose for which it will be used may remain unknown. In addition, data subjects cannot retrieve, correct, control or delete such data if they are unaware it exists.

## PRO: Biometric Data Collection Impacts Millions

Civil Liberties Union for Europe, August 3, 2021

https://www.liberties.eu/en/stories/pros-and-cons-of-facial-recognition/43708

Such incredibly private information is currently being used by law enforcement to make policing decisions, and might in the future be employed by public or private bodies to make decisions as to e.g. your suitability for a job, a university course or loans, overseas travel, or entry into a festival.

# **Security Concerns**

# PRO: Avoiding Data Breaches/Vulnerabilities

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

The facial imprints and videos require bulk storage, due to which the security concerns tend to rise as the databases are quite vulnerable and can easily be breached. A large number of cases are reported regarding the database breaches in which the valuable facial scans were collected to use in finance corporations or police departments.

#### PRO: Data breaches

CEO World Magazine, May 9, 2022

https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/

Just like other forms of data, biometric technology is precious. As many companies now rely on biometrics and store data surrounding it, it's possible that they then become targets for malicious third parties. Another thing to consider is that biometric data cannot be replaced. Once the hackers gain access to something, it will be challenging to get them out, unlike simply resetting a password.

#### PRO: not always accurate

CEO World Magazine, May 9, 2022

https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/

It might not always be accurate. While biometric systems are generally accurate, there could still be issues when logging into anything. Some smartphone users have reported that it's difficult for them to unlock their phones when there's a bit of dirt on their fingers which can be annoying, while others have claimed that wearing glasses has prevented them from unlocking their phones. Biometric technology isn't always perfect.

# PRO: Deepfakes Fool Al

CX Today, June 3, 2021

https://www.cxtoday.com/contact-centre/weighing-the-pros-and-cons-of-voice-biometrics-technology/

Voice deep fakes are possible – Finally, audio deep fakes are becoming increasingly common and may be able to fool the Ai into believing the audio sample's veracity.

#### PRO: Police Still Have Sufficient Access

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

Privacy is considered the biggest issue in the cities like San Francisco, California, etc where law-abiding regulators have banned the usage of surveillance systems embedded with facial recognition technology. In suspicious cases, only law enforcement can record the videos or take photos from government allotted security video devices, but they lack the feature of face verification.

#### PRO: Data Breaches from Collecting Data (ex. 50m Users of Facebook!)

BBN Times, November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disquise

Social media platforms like Facebook and tech giants like Google and Apple have been at the center of the discussion pertaining to facial recognition privacy issues. Facebook, Google, and Apple can identify faces using artificial intelligence and machine learning and store the information in their internal databases. But Facebook's consistent use of state of the art machine learning, artificial intelligence, and big data can lead to negativity. By gathering personal details, recording every activity, check-in, likes and dislikes, Facebook can connect the gathered information with facial recognition technology to create a digital profile. Furthermore, companies to advertise products based on your data can use the digital profile. Recently, Facebook announced that the data of around 50 million users was compromised in a major security breach. The compromised data may contain phone numbers, email ids, personal details, and facial recognition information, which can easily get into the wrong hands.

# PRO: Risks from Outside Applications (ex. Smart Phones)

Harvard Business Review, December 6, 2017

https://hbr.org/2017/12/biometrics-wont-solve-our-data-security-crisis

As we begin to see the increased use of physical biometrics in interactions both where the consumer is present and not present, privacy concerns will invariably arise. While biometric data will typically reside on the smart phone or device itself, outside applications could easily tap the data for other uses allowed by the fine print of privacy policies and terms of use. Much like credit data, we could soon have a burgeoning cottage industry in what I call extrapolated uses of biometric data.

### PRO: Misuse of Data Collection

Harvard Business Review, December 6, 2017

https://hbr.org/2017/12/biometrics-wont-solve-our-data-security-crisis

Geolocation based behavioral biometric patterns can reveal exercise regimens (how often and how much time you spend at the gym) or work schedules (how much time you spend at the office) or when and where you go to the doctor or pick up your kids. Behavioral biometrics can become a passive watcher that triggers a flag when it recognizes a break in the usual pattern, similar to the expert systems that flag credit card fraud. It could be a powerful tool to root out identity thieves. The dark side of this approach is the potential misuse of its data collection by everyone from insurance companies to divorce lawyers.

### PRO: Data Breech Impacts School Children (ex. New York)

The Conversation, November 29, 2022

https://theconversation.com/as-more-biometric-data-is-collected-in-schools-parents-need-to-ask-these-10-questions-191263

Earlier this year in New York, about 820,000 public school students had personal information exposed after a cyber attack on a company that provides software to track grades and attendance. Biometric technology can easily be integrated into everyday edtech and school operations to manage things like attendance, exams and how students learn.

#### PRO: Biometric Technology Can Be Manipulated

Industry Today, February 21, 2023

https://industrytoday.com/facial-recognition-in-the-workplace-the-pros-and-cons/

Facial recognition can be prone to manipulation because the software relies on images. For example, if the system is designed to detect if someone has a beard, someone could easily alter their appearance by wearing a fake beard or putting on makeup that makes them appear older. In addition, cameras used for facial recognition may not be high-quality enough to identify people accurately.

#### PRO: Harm to Childrens' Security is 'Very Real'

The Conversation, November 29, 2022

https://theconversation.com/as-more-biometric-data-is-collected-in-schools-parents-need-to-ask-these-10-questions-191263

Why is this a problem? The UK's commissioner for biometric material Fraser Sampson is calling for a ban of biometrics in UK schools. As he said in a report this year: Harm is already very real [...] Further risks to the rights and freedoms, and full and free development of the child, may not be fully realized yet. This is similar to other calls in France and Sweden. We do not have enough independent research or a broad enough understanding of potential harms, which could range from privacy to security, identity theft, and infringements upon children's rights and freedoms.

## PRO: Biometric Errors Punish Innocent People

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

No systems are flawless and facial recognition is still in its infancy. There have been cases where people were wrongly accused of crimes based on misidentification. There can be people arrested that look similar to a criminal and may end up being found guilty of a crime they didn't commit. Because there is a risk of wrongful arrests and convictions, this technology should be used with caution and implemented as an additional source of the police investigation.\

## PRO: Theft of Biometric Data is Permanent

Civil Liberties Union for Europe, October 25, 2022

https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518

Biometric databases are widely used by police forces and governments, as well as popular websites and applications that store data on our faces or other biometric features such as our fingerprints. When Clearview AI, a notorious facial identification business that sells access to its database to, among other institutions, US law enforcement, US Senator Edward Markey stated: "If your password gets breached, you can change your password. If your credit card number gets breached, you can cancel your card. But you can't change biometric information like your facial characteristics."

### PRO: Security Vulnerabilities from Information Being Hacked

Civil Liberties Union for Europe, October 25, 2022

https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518

Facial images are extremely easy to collect because you can be filmed by cameras in public places. The biggest problem resides in the fact that no security system is airtight. Imagine there is a database with your photo or your address. If the database gets hacked and a malicious person gets access to it, they could use it for identity theft, robbery or harassment purposes. For instance, stalkers could perform reverse image searches on pictures to gather personal information about an individual, such as their address. They could also use your image to impersonate you online and scam people and police could think you are the person behind it.

# PRO: Facial Recognition Data Vulnerable to Breaches

Civil Liberties Union for Europe, August 3, 2021

https://www.liberties.eu/en/stories/pros-and-cons-of-facial-recognition/43708

Third, biometric data carries its own security risk. Unlike a password, biometric data cannot be changed. If my fingerprint data leaks, this is not something I can "reset" like a password. To make things worse, your face can be scanned anytime and anywhere, without your consent. This means that your biometric data might actually be stored in a range of databases, whose security measures might be inadequate.

# **Privacy Concerns**

PRO: Users' privacy

CEO World Magazine, May 9, 2022

https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/

While it's mostly secure, biometrics are anything but anonymous. Unlike passwords, you're literally at risk of having your identity known. When paired with other information about you, hackers could build a fake online identity about you. Biometrics could also be converted into data; sold by companies for a quick buck.

## PRO: Extremely Sensitive Privacy Issues

CX Today, June 3, 2021

https://www.cxtoday.com/contact-centre/weighing-the-pros-and-cons-of-voice-biometrics-technology/

Companies must be extremely sensitive about privacy and consent – Voice is innately personal and not every customer will be comfortable with sharing their voice data. Enforcing data privacy laws like GDPR can be problematic, as customer voice samples are relatively easy to collect. Already, the Chinese government has come under scrutiny for potentially breaching privacy rights and collecting voice pattern samples to build a national database.

#### PRO: Privacy Loss a Significant Downside

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

The biggest downside of the facial biometric is the significant threat to privacy. People discourage the idea of taking photos and storing them by an anonymous group which can be used in the future.

#### PRO: Surveillance State Threatens Freedom

BBN Times, November 02. 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

The most significant debate regarding the advanced facial recognition technology is revolving around facial recognition privacy issues. Civil rights groups are getting anxious after witnessing how capable artificial intelligence and machine learning are making the facial recognition technology. Furthermore, civil rights groups believe that facial recognition will lead to a surveillance state and eliminate the freedom of anonymity. The most commonly asked questions about facial recognition are, "Who is collecting the data?" "Where is the data being stored?" and "Who can access the data?"

#### PRO: Government Data for Tracking and Profiling

BBN Times, November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

While addressing facial recognition privacy issues, multiple technology experts have hinted that the government can track every move of their citizens, and create a database to store all the information without their permission. Additionally, the collected data can be used to profile individuals based on their face, behavior, and demographics.

## PRO: Violating Workers' Rights and Privacy

Industry Today, February 21, 2023

https://industrytoday.com/facial-recognition-in-the-workplace-the-pros-and-cons/

Some users have concerns about the privacy of facial recognition software. It can violate personal rights to monitor employees without their knowledge. Some companies are concerned that people will not want to work in an environment where they feel like they're being watched. This could cause morale issues and lead to a high turnover rate in the workplace.

# PRO: Scanning 97% of Airline Passengers (It's Mass Surveillance)

Stanford University's Cyber Policy Center, Stanford University, April 23, 2020

https://hai.stanford.edu/news/challenges-facial-recognition-technologies

Travel: U.S. customs relies on facial recognition for its biometric exit program, and 17 airports currently deploy the technology, with plans to scan 97% of departing passengers by 2024.

# **Privacy Concerns (Continued...)**

# PRO: Harm to Childrens' Privacy is 'Very Real'

The Conversation, November 29, 2022

https://theconversation.com/as-more-biometric-data-is-collected-in-schools-parents-need-to-ask-these-10-questions-191263

Why is this a problem? The UK's commissioner for biometric material Fraser Sampson is calling for a ban of biometrics in UK schools. As he said in a report this year: Harm is already very real [...] Further risks to the rights and freedoms, and full and free development of the child, may not be fully realized yet. This is similar to other calls in France and Sweden. We do not have enough independent research or a broad enough understanding of potential harms, which could range from privacy to security, identity theft, and infringements upon children's rights and freedoms.

## PRO: Tracking People Without Them Realizing

Stanford University's Cyber Policy Center, Stanford University, April 23, 2020

https://hai.stanford.edu/news/challenges-facial-recognition-technologies

We look at our phones to unlock our screens, tag friends in photos on social media, even validate our identities at ATMs by staring into the camera. At the same time, these technologies can track us in public settings, identify our criminal histories, and gauge our reactions to advertising, all beyond our notice. "Facial recognition technologies are widely deployed," says Marietje Schaake, international policy fellow at Stanford's Institute for Human-Centered Artificial Intelligence. "We don't always know it is happening."

#### PRO: Serious Consequences to Privacy

Stanford University's Cyber Policy Center, Stanford University, April 23, 2020

https://hai.stanford.edu/news/challenges-facial-recognition-technologies

Legal, Societal, and Policy Implications: As the use and power of this technology continues to expand, it raises a number of serious questions, Schaake notes. First, what are the consequences for privacy and anonymity? Should people have a presumption of privacy when they attend sporting events, take a walk in a public park, visit a hospital, or pick up our child at school? "What one person might think is legitimate use, another person might think of as abusive or a blanket violation of rights," she says.

## PRO: Facial Recognition Violates Privacy

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

People don't want their identity recorded and stored without their permission, and facial recognition can be seen as violating their privacy. If your picture is run through criminal databases, it is like treating people as suspects without probable cause.

#### PRO: Infringement on individual privacy

Civil Liberties Union for Europe, October 25, 2022

https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518

The way facial recognition technology is used is inherently invasive and intrusive. As it is done today, data collection is realized without the consent or the knowledge of the individuals: for instance, you can be filmed just walking down the street. Being recorded and monitored without one's consent and even knowledge is a clear infringement of one's individual privacy and freedom. It takes away the reassurance of being able to move and act freely without the fear of being constantly watched and surveilled. Being watched changes the way we behave and also affects our well being. Such a gaze may create a feeling of always being surveilled by people, which can lead to increased stress and decreased trust between the people and the government. If people fear their daily interactions and conversations are being monitored, they might avoid criticizing the government for fear of something happening to them or their loved ones.

# **Privacy Concerns (Continued...)**

PRO: Facial Recognition Collects Without Consent

Civil Liberties Union for Europe, August 3, 2021

https://www.liberties.eu/en/stories/pros-and-cons-of-facial-recognition/43708

Worryingly, more often than not our images are uploaded to facial recognition databases without our awareness or consent. For example, it has recently been discovered that Clearview AI, a US technology firm, scraped over three billion facial images from social media platforms such as Facebook, YouTube and Twitter, and gave access to our data to governments and private firms in exchange for payments.

# **Violating Civil and Human Rights**

# PRO: Facial Recognition "Chills" Freedom (& Rights)

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

The feeling of being watched and your movements monitored will affect people's behavior. No one wants to be recorded, and if you fear being watched, you may not want to go out or frequent a store or public place that uses facial recognition.

## PRO: Infringement on Freedom of Speech from Mass Surveillance

Civil Liberties Union for Europe, October 25, 2022

https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518

Facial recognition technology is of concern because of its potential to become a biometric mass surveillance tool. Surveillance, especially in the case of demonstrations, muzzles freedom of expression and chills activities such as political activism. These tools are used to monitor the population and, in countries where criticizing the government is not tolerated, to the arrest of those who oppose the government. In the USA, the NGO Electronic Frontier Foundation exposed the fact that the San Francisco Police Department gained live access to over 400 cameras to spy on protestors during the 2020 protests. When certain technologies are in places, they can be, and often are, misused.

#### PRO: Violating Presumption of Innocence

Civil Liberties Union for Europe, October 25, 2022

https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518

Surveillance of people on the basis that they might do something illegal in the future is also an infringement of the presumption of innocence. Law enforcement could treat someone differently on the basis of a supposed future culpability, which cannot be proven.

# PRO: Infringing on 1st Amendment Freedoms (ex. Chills Speech/Assembly)

Civil Liberties Union for Europe, October 25, 2022

https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518

In a VICE article, Joshua Franco, senior research advisor and the deputy director of Amnesty Tech at Amnesty International stated: "The fear and uncertainty generated by surveillance inhibit activity more than any action by the police, [...] if you feel you're being watched, you self-police, and this pushes people out of the public space."

### PRO: Using Facial Recognition Data is Intrusive

Civil Liberties Union for Europe, August 3, 2021

https://www.liberties.eu/en/stories/pros-and-cons-of-facial-recognition/43708

Facial recognition fails to respect our rights in more than one way. First, the technology intrusively acquires some of our most intimate data. Because our data belongs to us, (e.g. under the General Data Protection Regulation), we have the right to know when personal information is obtained about us & for which purpose.

### PRO: Using Facial Recognition Data Threatens Freedoms (ex. Intimidation)

Civil Liberties Union for Europe, August 3, 2021

https://www.liberties.eu/en/stories/pros-and-cons-of-facial-recognition/43708

Second, knowing that we can be easily identified can lead us to self-censor for fear of negative consequences. For example, people who know that they will be identified and placed in a database for showing up at a protest may be put off attending. This is especially damaging in situations where governments have illegally restricted the right to demonstrate to stifle public criticism.

#### **Discrimination/Racism Concerns**

#### PRO: Risks of Discrimination and Racial Bias

CX Today, June 3, 2021

https://www.cxtoday.com/contact-centre/weighing-the-pros-and-cons-of-voice-biometrics-technology/

There is a risk of discrimination and racial bias – As mentioned, voice biometrics algorithms (especially those used for identification and not verification), have to be trained on comprehensive datasets, comprising a diverse range of human voices. But studies suggest that the dataset used for training most mainstream voice technologies might be racially skewed, which makes the AI better at recognizing some demographics than others.

# PRO: Increased Risk of False Allegations (Due to Misidentification)

Industry Today, February 21, 2023

https://industrytoday.com/facial-recognition-in-the-workplace-the-pros-and-cons/

Despite being more accurate than the human eye, facial recognition technology is still not 100% perfect. The software may struggle to identify people with dark skin and those with similar facial features, in the case of identical twins, or those wearing makeup that obscures their natural appearance. If the software misidentifies someone, it could lead to false accusations of theft or fraud.

#### PRO: Misidentification and Racial Bias

Stanford University's Cyber Policy Center, Stanford University, April 23, 2020

https://hai.stanford.edu/news/challenges-facial-recognition-technologies

Another issue of growing concern is bias, when software that's often trained on white, male images frequently misidentifies women and people of color.

#### PRO: Racial Bias in Data Causes Misidentification

Civil Liberties Union for Europe, October 25, 2022

https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518

Survey results demonstrate that this technology, as all others, was not immune to judgmental bias. It recognizes white men more readily than women or other ethnic groups. In 2018, 35% of facial recognition errors happen when identifying women of color, compared to 1% for white males. This bias was reduced through training over time, but it is still there and very difficult to eradicate completely.

### PRO: Misidentification Leads to Discrimination & False Arrest

Civil Liberties Union for Europe, October 25, 2022

https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518

These false positives can turn into false arrests. Nijeer Parks, for example, was arrested in 2019 in the USA for allegedly shoplifting and trying to hit an officer with a car. He had been misidentified and wrongfully arrested based on facial recognition. The case was dropped eventually but it took a year, including 10 days in jail and 5000\$ spent on legal defense. In addition, the use of biometric information with the aim of classification on certain criteria could pave the way for profiling, resulting in discrimination and wrongful convictions against certain groups because of conscious or unconscious biases in the justice system.

### PRO: Discrimination Against "People of Color"

Civil Liberties Union for Europe, August 3, 2021

https://www.liberties.eu/en/stories/pros-and-cons-of-facial-recognition/43708

Not only does face recognition discriminate against people of color, but it is also disproportionately targeted at marginalized individuals. In a law enforcement context, facial recognition is predominantly used in communities that are already over-policed. In Italy, for instance, the police's facial recognition software database contained 2 million images of Italians, compared to 7 million of refugees and migrants. So the way this technology is used is likely to perpetuate the way people from some groups are already disproportionately targeted.

# **Discrimination/Racism Concerns (Continued...)**

# PRO: Facial Recognition Technology Threatens Minorities

Civil Liberties Union for Europe, August 3, 2021

https://www.liberties.eu/en/stories/pros-and-cons-of-facial-recognition/43708

Facial recognition technology is also known to work relatively well on white and male faces, while having a high rate of inaccuracy on people of color, especially if they are female. This means that people from ethnic minority groups, who already tend to have less easy access to services and amenities, will encounter an extra barrier when authorities use facial recognition in these contexts.

# **Businesses Exploit Workers & Customers**

## PRO: Companies Collecting Data for Exploiting Customers

BBN Times, November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

Social media platforms like Facebook and tech giants like Google and Apple have been at the center of the discussion pertaining to facial recognition privacy issues. Facebook, Google, and Apple can identify faces using artificial intelligence and machine learning and store the information in their internal databases. But Facebook's consistent use of state of the art machine learning, artificial intelligence, and big data can lead to negativity. By gathering personal details, recording every activity, check-in, likes and dislikes, Facebook can connect the gathered information with facial recognition technology to create a digital profile. Furthermore, companies to advertise products based on your data can use the digital profile. Recently, Facebook announced that the data of around 50 million users was compromised in a major security breach. The compromised data may contain phone numbers, email ids, personal details, and facial recognition information, which can easily get into the wrong hands.

#### PRO: Tracking People Without Them Realizing

Stanford University's Cyber Policy Center, Stanford University, April 23, 2020 <a href="https://hai.stanford.edu/news/challenges-facial-recognition-technologies">https://hai.stanford.edu/news/challenges-facial-recognition-technologies</a>

We look at our phones to unlock our screens, tag friends in photos on social media, even validate our identities at ATMs by staring into the camera. At the same time, these technologies can track us in public settings, identify our criminal histories, and gauge our reactions to advertising, all beyond our notice. "Facial recognition technologies are widely deployed," says Marietje Schaake, international policy fellow at Stanford's Institute for Human-Centered Artificial Intelligence. "We don't always know it is happening."

#### Cost and Economic Concerns

#### PRO: Tremendous Costs

CEO World Magazine, May 9, 2022

https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/

To maintain and sustain a strong security profile, companies will have to spend significant money to ensure software and hardware are up to date. Beyond companies, biometric security can also be expensive for personal use. Prices for biometric access control systems like electronic doors and installation could cost upwards of 2,500 U.S. dollars.

### PRO: Increased Storage Requirements (& Costs)

BBN Times, November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

Storage space for all the images and videos is one of the significant issues with the facial recognition technology. Additionally, enrolling faces into the recognition software requires extra space for every new employee. HD quality images are known to produce error-free results, but increase the storage requirements of the system.

#### PRO: Failure to Delete Biometric Data (ex. Texas vs. Google)

CUSO Magazine, January 30, 2023

https://cusomag.com/2023/01/30/the-risks-and-rewards-of-biometric-data/

At the end of 2022, two cases helped illustrate some of the risks when acquiring biometric data. In October 2022, the Attorney General sued Google on the basis of Google's alleged failure to (1) obtain informed consent from Texas citizens regarding the use of facial and voice biometric information through Google's applications, and (2) failure to delete the biometric information in a reasonable time. Texas is one of the states that regulate the capture, use, and disposal of biometric information, and this is the first lawsuit against a company under this law. Google faces civil penalties of up to \$25,000 per violation.

## PRO: Facial Recognition is Expensive (ex. Businesses Suffer)

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

There are costs to implementing a new security system. Installing cameras and buying computers with specific software to run tracking and maintain databases will be an extra cost for businesses. There is also staff that will need to operate and maintain this equipment.

## PRO: Facial Recognition Wastes Taxes & Causes Inflation

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

For use in law enforcement and gov't. security measures, that cost will be paid through tax dollars. It will drive up the price of goods and services at airports and businesses.

# BANNING BIOMETRIC DATA COLLECTION WILL NOT BE EFFECTIVE (CON)

Effectiveness (ex. No Need, Ban = Ineffective, & Regulations = Preferable)

CON: Current Laws and Lawsuits Prevent Abuse (No Need for Ban!)

CUSO Magazine, January 30, 2023

https://cusomag.com/2023/01/30/the-risks-and-rewards-of-biometric-data/

The collection of biometric information is becoming more prevalent in the credit union industry and in fintech as a whole. Consumers cannot easily change biometric information about themselves; therefore, theft of biometric information is among the most serious of all data breaches. As a result, several states have enacted laws regulating the capture and storage of biometric data. Even in states without laws specifically relating to biometric information, loss of biometric data can result in negligence lawsuits against the organization that held the data.

## CON: Many States Considering/Pursuing Regulations

CUSO Magazine, January 30, 2023

https://cusomag.com/2023/01/30/the-risks-and-rewards-of-biometric-data/

Three states currently have laws that directly regulate consumer biometric information: Illinois, Texas, and Washington. Of these, Illinois has the most stringent requirements and also allows consumers to file a class action lawsuit for violation of the law. Texas and Washington, by contrast, require any lawsuit to be filed by the state attorney general. Six other states, Arkansas, California, Colorado, Maryland, New York, and Virginia, have privacy laws that while not biometric specific likely require protection of biometric data if captured and stored. Many other states are considering laws that imply or directly regulate the capture and use of biometric data.

#### CON: Regulations are Key (ex. Banning is too Extreme!)

BBN Times, November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

The on-going debate around facial recognition privacy issues represents both the extremes of the spectrum. Governments should apply regulations to avoid malicious applications of facial recognition and curb any chances of creating a surveillance state. Facial recognition should only be used to improve the security of every individual and other ethical practices.

### CON: Increased Regulation for Biometric Data Collection

Epig Global, Last Accessed: April 2023

https://www.epigglobal.com/en-us/resource-center/articles/more-businesses-using-biometric-data

So, what should litigators and organizations handling biometric data be doing this year? Ramping up compliance efforts, monitoring relevant court decisions, and tracking legislative process outside of Illinois will be key. While BIPA can apply outside Illinois, new state laws that pass would add to the dominance of biometric litigation. The correlation of more biometric data collection and increased regulatory attempts nationwide signifies the importance of how data trends drive legal action. Facial recognition will definitely be a continued focus and new trends will undoubtedly materialize. Organizations must understand their risk with biometric data collection so they can close gaps and stay ahead of the curve.

# CON: Lawsuits Hold Companies/Governments Accountable

Epig Global, Last Accessed: April 2023

https://www.epigglobal.com/en-us/resource-center/articles/more-businesses-using-biometric-data

There are notable underlying themes. Courts are continuing to interpret BIPA broadly to put organizations on notice about unacceptable data hygiene practices. It does not take much to establish a cause of action, the potential plaintiff pool is wide in class actions, statute of limitations is longer, damages can be massive, and liability is expanding to third-party actions. The explosion of BIPA litigation seen over recent years will not slow down anytime soon, so organizations need to regularly evaluate their exposure risk and take steps to mitigate proactively. Failure to do so could result in BIPA-related litigation costs and monetary liability.

# Effectiveness (Continued...)

CON: Data Not Intended for Malicious Purposes (ex. Security is the goal)

BBN Times, November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

The response given by people who advocate the use of facial recognition is that if one has nothing to hide, then there's no reason to be worried. While addressing the facial recognition privacy issues, governments and technology giants constantly assure that they are not using the facial recognition technology for surveillance or any other malicious purposes. Additionally, governments ensure that facial recognition makes workplaces and public places more secure.

# CON: Abandoning New Technologies is Ridiculous (No Malicious Intent!)

BBN Times, November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

However, it can be argued that any type of technology can be used for malicious activities if one intends to do so. Hence, the argument that the technology should be abandoned altogether becomes ridiculous. Not all technology giants would introduce new technologies; invest in research and development, with the sole intent of surveillance or other malicious activities. On the other side of the argument, the worst-case scenarios with new technologies must be well thought through, to prepare for handling them. In conclusion, we need to be more open-minded with new technologies as they have the potential to create a better future and also be cautious of the unwarranted impact they may create.

#### CON: Increased Efficiency and Accuracy

Industry Today, February 21, 2023

https://industrytoday.com/facial-recognition-in-the-workplace-the-pros-and-cons/

Facial recognition technology can scan and identify faces in just seconds. This is an improvement over manual processes, which may take minutes to review and verify a person's identity. The human eye may also not be the most accurate tool in identifying people, which is why facial recognition technology is preferred. Lastly, it's more reliable than biometric security measures such as fingerprint and iris scanners. This is because the human face is harder to replicate.

# CON: Punishment Prevents Abuse (ex. Facebook & Clearview Al)

Stanford University's Cyber Policy Center, Stanford University, April 23, 2020

https://hai.stanford.edu/news/challenges-facial-recognition-technologies

As governments are working on laws to protect their citizens, a number of court cases have already challenged the technology. Facebook settled a lawsuit in Illinois for \$500 million for harvesting users' photos without consent. The attorney general of Vermont sued Clearview AI for collecting photo information without permission, and the ACLU is suing several law enforcement agencies, including the Department of Homeland Security and Immigration and Customs Enforcement, to obtain information over their use of facial recognition software.

# **Security Concerns**

**CON: High-security assurance** CEO World Magazine, May 9, 2022

https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/

Because biometrics rely on fingerprints, irises, and other unique human features, they can be a better option than passwords for protecting accounts. When paired with other forms of multi-factor authentication (MFA), you can also add another layer of security that is more difficult for others to hack. Because biometric authentication generally requires a living, breathing human to be present, it can be pretty tricky for Al or other forms of technology to spoof. Most times, biometric authentication can work in low-light conditions.

#### CON: Difficult to fake

CEO World Magazine, May 9, 2022

https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/

As mentioned earlier, biometric technology is relatively hard to fake and spoof. While not impossible, facial patterns, irises, and fingerprints are difficult to replicate and could take more effort than necessary. While some phones can be unlocked with photos, consumer technology companies can prevent this by improving their technology in general. For example, most smartphones use 2D facial recognition scanning technology. Still, in the future, more smartphones might adopt 3D facial recognition instead to make it even harder for hackers to spoof things.

### CON: Deepfakes Extremely Difficult

CX Today, June 3, 2021

https://www.cxtoday.com/contact-centre/weighing-the-pros-and-cons-of-voice-biometrics-technology/

A person's voiceprint is extremely hard to spoof – In an identity theft case, a fraudster can get hold of a customer's date of birth, address, and unique information like their mother's maiden name or the name of their first pet. However, every individual has a distinct voiceprint, which is far harder to obtain or mimic.

#### CON: Improving Safety in Public Spaces (ex. Banks, Airports)

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

The facial biometric is a vast spread in the domain of finance and travel. It is the source of improving the safety as well as the security measures in retail sectors such as airports and banks. Customer screening is an integral part of airport security.

### CON: Preventing Illegal Activities (ex. Airport and Border Security)

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

This works the same as identifying the criminals from public places, the biometric technology is helping out to determine the customers which pose the potential threats which can impact airlines as well as the passenger. In addition, it's quite beneficial for security agencies to verify the individuals requesting to cross the border.

### CON: Enhanced Financial Security (ex. Preventing Bank Fraud)

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

Financial institutes like banks are also using biometric technology to enhance the security checks to prevent frauds and to determine the customer who was charged before for any of the potential crimes.

### **CON: Biometrics Necessary to Catch Criminals**

Tech Research Online. September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

Government and law enforcing agencies have widely been using face biometric technology to identify the criminals which tend to be "ghosting" whereas there is no other way of determining such people.

# CON: Liveness Detection & Protection

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

The facial biometric verification mechanism has various features to ensure security and prevent impersonators from causing any trouble to the system. Following are some of the common features that facial recognition software provides: During the process of verification, liveness detection checks prevent any chances of spoof attacks by ensuring the live presence of the user. Fraudsters tend to deceive biometric verification checks as well but liveness detection analysis enables you to identify and eliminate such attempts beforehand.

### CON: 3D Depth-Sensing Protections

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

The facial biometric verification mechanism has various features to ensure security and prevent impersonators from causing any trouble to the system. Following are some of the common features that facial recognition software provides: These checks are crucial to ensure that the image is not tempered with the ID document. It scans the different points on the image and compares them against previously saved digitized images. 3D facial recognition, AI, & human intelligence used collectively for this check.

### CON: Deepfake Detection & Protection

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

The facial biometric verification mechanism has various features to ensure security and prevent impersonators from causing any trouble to the system. Following are some of the common features that facial recognition software provides: The facial recognition system cross-checks the user's photo with the picture on his ID document submitted at the time of verification. It uses AI mapping techniques, image distortion analysis, and micro expression checks to detect any kind of deep fakes and 3D masks spoofing measures. In case of a suspicious attempt, the system declines the verification status of the user and eliminates the impersonation efforts.

#### CON: Deterring Criminals (ex. ID Theft)

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

The facial biometric systems with multi-factor authentication are effective countermeasures for finding missing people, increasing security surveillance at the airport, or cross-border checks. It provides an additional layer of security to deter the increasing number of identity thefts.

#### **CON: Numerous Security Protections**

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

Robust 3D facial recognition techniques such as Al mapping, liveness detection, and microexpression analysis detect and eradicate spoofing attempts made through deep fakes, photoshopped or distorted images, and 3D masks. There are numerous benefits of facial recognition technology.

### CON: Unparalleled Effectiveness

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

Developed in the 1960s, facial recognition has become more accurate and advanced with time by employing several artificial intelligence algorithms. Facial recognition is one of the best biometric systems that identify the user by capturing his live selfie and matching it against other images in the database. It can address more sophisticated security challenges with unparalleled efficacy, sensitivity, and perception.

# CON: Avoiding Errors in Identifying Criminals/Terrorists

BBN Times, November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

Law enforcement can use facial recognition and AR to help identify criminals. The mug shots of criminals are compared to the mug shots in the police database to recognize repeat offenders. Additionally, law enforcement can use Al-powered facial recognition to find missing children. Today, high definition cameras can be used to look for terrorists in public places based on internal information in the police database. Deploying artificial intelligence and machine learning with facial recognition avoids the chances of errors when it comes to recognizing criminals.

# CON: Hack Proof ID (ex. Experts Failed vs Apple iPhone)

BBN Times, November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

Imagine a world where you can pay for your cereal without cash, cards, or a phone, by just smiling at the cashier. Now, imagine being monitored by the authorities for being an ethnic minority. From smiling to pay to being monitored as an ethnic minority, countries worldwide are displaying both, the bright as well as the dark sides, of using the facial recognition technology. Facial recognition is not an altogether new technology, but artificial intelligence and machine learning are constantly making facial recognition better. Apple raised the bar for facial recognition by introducing the facial biometric system with 3D scanning with iPhone's Face ID. In fact, iPhone's face ID is so accurate that WIRED attempted to spoof or hack the face ID with the help of experts, but failed miserably. While modern technology is making facial recognition more accurate and secure, concerns related to facial recognition privacy issues and surveillance are also being raised. So, let's explore the pros and cons of this buzzing technology in this post.

#### **CON: Biometrics Provide Enhanced Security**

BBN Times, November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

With the 3D biometric system and infrared cameras, facial recognition can perform more efficiently. A company's premises can be secured by monitoring employees and visitors. Moreover, trespassers can be identified immediately. As a result, facial recognition can drastically improve security & safety at workplaces.

## CON: Biometrics Produce High Accuracy

BBN Times. November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

With artificial intelligence and machine learning, facial recognition has achieved a higher success rate. Hence, the chances of spoofing the system or hacking are severely reduced. Now, security systems can precisely identify people that are illegitimately entering private properties and notify concerned authorities.

#### CON: Reducing Fraud-Based Crimes

CUSO Magazine, January 30, 2023

https://cusomag.com/2023/01/30/the-risks-and-rewards-of-biometric-data/

Biometric data has real value in the fintech industry. Properly used, fintech helps reduce the risk of fraud-based crimes such as identity theft or money laundering. Biometrics are also ideal for protecting sensitive financial transactions. Financial institutions and CUSOs should not strive to avoid biometrics altogether, which is becoming increasingly impossible in any event, but rather be aware of the laws around the use of biometric data and ensure the common requirements of state laws are met. Credit unions are already proficient in protecting the financial information of their members, and applying those practices to biometrics can ensure less fraud and a better experience for their members.

# CON: Higher Security for Less Cost

CUSO Magazine, January 30, 2023

https://cusomag.com/2023/01/30/the-risks-and-rewards-of-biometric-data/

Despite the risk, biometric authentication has a number of advantages, and the use of biometric data is likely to accelerate. For example, with the push to multifactor authentication ("MFA"), biometric identifiers check the box of "something a person has" and helps verify identity. User experience is often convenient and fast, and while not perfect, biometric identifiers are much harder to steal than passwords. Biometric data can be cheaper to store and use, for example by not incurring charges commonly associated with MFA, such as the costs of texting a code to a user's phone.

### CON: Identifying Serious Threats Quickly

Industry Today, February 21, 2023

https://industrytoday.com/facial-recognition-in-the-workplace-the-pros-and-cons/

Facial recognition technology can quickly identify threats in crowded areas, such as airports or stadiums. This is especially important for airports, where TSA agents must screen thousands of passengers rapidly. The technology also helps to quickly identify criminals and terrorists by scanning faces against a database of known offenders. This is especially useful for law enforcement agencies trying to keep track of people who are banned from entering certain areas.

### CON: Making Schools Safer

Stanford University, April 23, 2020

https://hai.stanford.edu/news/challenges-facial-recognition-technologies

Education: Some public school systems in the U.S. are implementing the technology to track people who have been banned from campus or to record class attendance.

#### CON: Facial Recognition Identifies Criminals (via CCTV)

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

Law enforcement agencies can use facial recognition to help identify criminals using live CCTV cameras to map faces and compare them to their databases. Wanted lists can be quickly scanned to find positive matches, which will speed up the apprehension and prosecution of felons.

# CON: Facial Recognition Significantly Improves Security

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

Video face recognition can be used to identify criminals and other threats like weapons. It can detect people using surveillance, so security guards can stop entrance into businesses, events or other private spaces. If a business is burglarized, the software may also help identify and track thieves. Airport security screening has implemented this technology, and it can scan their high-traffic areas of people to find known criminals travelling.

### CON: Facial Recognition Improves Personal Security

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

Facial recognition is used as a tech password for devices like computers, tablets and smartphones, too, making it impossible to gain access to someone's electronics.

### CON: Facial Recognition Reduces Security Risks

Foundation for the Future. January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

Facial recognition helps with security because key cards can get stolen and allow anyone to enter a building. Passcodes may be shared, letting multiple people use them for unlawful entry. Facial recognition eliminates this.

CON: Increased Reliability in Personal Security (ex. No Passwords)

Civil Liberties Union for Europe, August 3, 2021

https://www.liberties.eu/en/stories/pros-and-cons-of-facial-recognition/43708

While the internal processes for biometric authentication are technical, from a user's point of view it's incredibly easy and quick. Placing a finger on a scanner and unlocking an account in seconds is faster than typing out a long password that has multiple special characters. In addition, forgetting a password is a common mistake of most users. The chances of you forgetting your own biometrics? 0%!

# CON: Biometrics Can Improve Security

Civil Liberties Union for Europe, August 3, 2021

https://www.liberties.eu/en/stories/pros-and-cons-of-facial-recognition/43708

Another argument is that facial recognition helps ensure security. Biometrics are said to provide increased levels of assurance that a person trying to access a service or make a transaction is real. Those in favour of using biometrics point out that passwords, PINs and other personal identifying information can be compromised by data breaches, allowing fraudsters to access accounts that use traditional authentication methods. In contrast, it's more difficult for someone other than you to provide your fingerprint on the spot. When it comes to law enforcement, those favoring facial recognition argue that it allows the police to track down suspects more easily.

## **Hurting Businesses**

# CON: Increased Quality of Customer Experience

CX Today, June 3, 2021

https://www.cxtoday.com/contact-centre/weighing-the-pros-and-cons-of-voice-biometrics-technology/

Its convenience helps the quality of CX – Voice-biometrics-based authentication is more convenient for the customer than physically entering a password, remembering answers to secret questions, etc. There is no dependence on memory or recall, as your voice itself acts as the identifier.

#### **CON: Excellent Candidate for Automation**

CX Today, June 3, 2021

https://www.cxtoday.com/contact-centre/weighing-the-pros-and-cons-of-voice-biometrics-technology/

It is an excellent candidate for automation – Voice biometrics can be used to automatically obtain a person's approval after verifying their identity. For instance, a live agent doesn't need to ask a customer for consent before recording a call – an automated IVR can request, while voice biometrics verifies that it was indeed the customer who provided their consent.

### **CON: Automation Reduces Chance of Errors**

BBN Times, November 02, 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

Instead of hiring security officials to identify people, facial recognition technology can make the process automated. Manual recognition can be a tedious process and introduces the chances of errors. However, facial recognition works 24/7, recognizes faces automatically, and provides more reliable results.

### CON: Biometric Data Improves Workplace Productivity

Industry Today, February 21, 2023

https://industrytoday.com/facial-recognition-in-the-workplace-the-pros-and-cons/

This ensures that employees are not slacking off or spending too much time on non-work activities. Facial recognition technology can be used to track where employees are at any given time, which helps managers keep tabs on their staff and ensure that everyone is doing their job. This also makes it easier to find out who has been late for work or failed to show up for work and when an employee leaves the facility after their shift.

### **CON: Improved Workplace Security**

Industry Today, February 21, 2023

https://industrytoday.com/facial-recognition-in-the-workplace-the-pros-and-cons/

The use of facial recognition technology can improve security in the workplace. It can be used to verify the identity of employees as they enter and leave work, which helps ensure that only authorized personnel are present during working hours. It also makes it easier to discover when unauthorized people come into the facility by comparing their faces against a database of authorized employees. This is especially useful for companies dealing with sensitive data such as financial and medical records.

#### CON: Preventing Theft and Fraud

Industry Today, February 21, 2023

https://industrytoday.com/facial-recognition-in-the-workplace-the-pros-and-cons/

Businesses can use facial recognition technology to prevent theft and fraud. This is especially useful in retail stores, where employees can access a lot of merchandise. The software can monitor the behavior of both customers and employees, ensuring that no one tries to steal from the company or sell products at a higher price than the management set.

## **Undermines Rescue Efforts (ex. Human Traffickers)**

# CON: Rescuing Children from Human Traffickers

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

On another hand, the lost people are also easily identified by comparing their facial imprints using live camera feeds against the global watchlists. This technology is also aiding in finding the children that are victims of human trafficking.

## CON: Helpful for Identifying Lost Children

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

Artificial intelligence-based facial recognition technology is embedded into the aging software which draws the image of kids, portraying how the children would be looking in coming years, and by comparing with the present image police are able to determine such potential matches.

#### CON: Facial Recognition Locates Missing Persons

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

When a person goes missing, especially a child, the faster they are found, the better, anything that aids in their recovery should be used, and facial recognition works in real-time. Any matches picked up on cameras can be quickly followed, given the location and time they were in the location. There are also databases where people can upload pictures of suspected missing persons and verify them. Implemented ageing software can also aid in helping find abducted children that have been missing for years.

### **Loss of Convenience**

## CON: Convenience - Easy to use

CEO World Magazine, May 9, 2022

https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/

Biometric technology is straightforward to use. While they're primarily found in high-security spots, like airports, hospitals, and similar, everyday items like smartphones, tablets, and laptops utilize biometrics. Both Android and iOS devices use different forms of biometric technology, such as fingerprint and facial scanning, which means users no longer have to type out a passcode to access their phones. Some financial and messaging apps, too, use biometric technology to allow users to gain access instead of typing out their passwords. This makes the user experience surrounding biometric technology so much more appealing.

## CON: Easy to integrate

CEO World Magazine, May 9, 2022

https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/

Many software applications use biometrics, and because it's available for use across multiple platforms, it's relatively easy to secure your accounts in just one tap. Those with smart homes will also appreciate how easy it is to integrate biometrics into several IoT devices at home.

#### CON: Facial Recognition Improves Efficiency

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

An advantage of facial recognition is its ability to identify people at an airport. The technology can detect your identity quickly instead of checking a passport, which will save time. Long lines can be reduced, and the whole system becomes more efficient. This can be implemented in other areas like bank machines. It can speed up business transactions by making payments using biometrics instead of regular methods.

# **Undermining Help for Vulnerable Groups (ex. Health, Homeless, & Welfare)**

## CON: Undermining Health Treatments

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

Biometric technology is also aiding healthcare, surprisingly it's mainly used in the detection of genetic disorders. By examining the facial traitor of the patient, a biometric recognition solution can identify the genetic mutation pattern which is causing the syndrome. Biometric technology is faster and less expensive is used as compared to the traditional test.

### CON: Identifying Patients and Diagnosis

Stanford University's Cyber Policy Center, Stanford University, April 23, 2020

https://hai.stanford.edu/news/challenges-facial-recognition-technologies

Health care: Facial recognition software can identify patients and diagnose genetic conditions.

### CON: Protecting Vulnerable Groups (ex. Homeless, Welfare, Etc.)

Stanford University's Cyber Policy Center, Stanford University, April 23, 2020

https://hai.stanford.edu/news/challenges-facial-recognition-technologies

Social services: Some homeless shelters have experimented with the technology to help identify people seeking services who don't have other forms of identification.

### CON: Facial Recognition Reduces Spread of Disease

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

As we are worried about touching surfaces, facial recognition can replace pin pads and key cards. We are more concerned than ever about spreading disease, so having a recognition method without touching a device is good.

# CON: Biometrics Increase Efficiency

Civil Liberties Union for Europe, August 3, 2021

https://www.liberties.eu/en/stories/pros-and-cons-of-facial-recognition/43708

Face recognition is promoted as something that makes our lives more convenient. Instead of having to bother entering a password into our phone, for example, or needing to show our ID at an airport, our faces will be enough to verify who we are. In Osaka at four train stations facial recognition systems were implemented to let people pass just by scanning their faces, without using a ticket or an ID card. A transport official noted that they would "emphasize as an advantage the fact that passengers with large luggage will be able to pass gates simply by showing their faces instead of looking for tickets".

#### **BIBLIOGRAPHY**

## Pros and Cons of Biometrics,

CEO World Magazine, May 9, 2022

https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/

## Facial Recognition: PROS & CONS of Regulating Biometric Technology,

Congressional Digest, April 2020

https://congressionaldigest.com/issue/facial-recognition/

#### The Pros and Cons of Voice Biometrics Technology,

CX Today, June 3, 2021

https://www.cxtoday.com/contact-centre/weighing-the-pros-and-cons-of-voice-biometrics-technology/

## Pros and Cons of Facial Recognition - Everything You Need to Know,

Tech Research Online, September 2, 2021

https://techresearchonline.com/blog/pros-and-cons-of-facial-recognition/

# Pros and Cons of Facial Recognition - Is it a Blessing or a Curse in Disguise?,

BBN Times. November 02. 2022

https://www.bbntimes.com/technology/pros-and-cons-of-facial-recognition-is-it-a-blessing-or-a-curse-in-disguise

## The Risks and Rewards of Biometric Data,

CUSO Magazine, January 30, 2023

https://cusomag.com/2023/01/30/the-risks-and-rewards-of-biometric-data/

#### Biometrics Won't Solve Our Data-Security Crisis

Harvard Business Review, December 6, 2017

https://hbr.org/2017/12/biometrics-wont-solve-our-data-security-crisis

### Facial Recognition in the Workplace: The Pros and Cons,

Industry Today, February 21, 2023

https://industrytoday.com/facial-recognition-in-the-workplace-the-pros-and-cons/

#### As more biometric data is collected in schools, parents need to ask these 10 questions,

The Conversation, November 29, 2022

https://theconversation.com/as-more-biometric-data-is-collected-in-schools-parents-need-to-ask-these-10-questions-191263

# More Businesses Using Biometric Data Means More Regulation,

Epig Global, Last Accessed: April 2023

https://www.epigglobal.com/en-us/resource-center/articles/more-businesses-using-biometric-data

#### The Challenges of Facial Recognition Technologies,

Stanford University's Cyber Policy Center, Stanford University, April 23, 2020

https://hai.stanford.edu/news/challenges-facial-recognition-technologies

# 8 Pros and Cons of Facial Recognition: Impact on Society,

Foundation for the Future, January 26, 2022

https://www.foundationforfuture.org/8-pros-and-cons-of-facial-recognition-on-society/

# 7 Biggest Privacy Concerns Around Facial Recognition Technology,

Civil Liberties Union for Europe, October 25, 2022

https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518

#### Facial Recognition: Pros and Cons.

Civil Liberties Union for Europe, August 3, 2021

https://www.liberties.eu/en/stories/pros-and-cons-of-facial-recognition/43708