Using Facial Recognition to Identify Persons of Interest at Large, Private Events, While Protecting Personal Data and Privacy

By

Dwight Lin

Critical Challenge Project

Submitted in partial fulfillment of the requirements for the
Degree of Executive Master in Cybersecurity
in the School of Professional Studies and
Department of Computer Science at Brown University

Project Advisor:

Deborah Hurley
Adjunct Professor of the Practice of Computer Science
Faculty Advisor

PROVIDENCE, RHODE ISLAND

MAY 2021

Abstract:

Facial recognition software has evolved a great deal within the past few years and its use as a security mechanism has become quite prevalent. A security value may be achieved from its application to identify persons of interest (POIs) at large scale, private events without necessarily causing undue burden to other attendees or their privacy. By combining facial recognition identification software and state-of-the-art video security systems (or CCTV), identification of persons of interests that pose a significant or credible threat or harm may be automated and enhanced to provide an additional layer of security. Implementing this technology, however, would require strict adherence to privacy and security standards. Securing facial recognition data and ensuring privacy necessitate strong privacy controls and cybersecurity measures that include notification, consent, data minimization, access control, authentication, encryption, and strict organizational policy.

This research paper provides a brief overview of facial recognition capabilities and limitations, current use cases, and presents a snapshot of the regulatory environment. It explores the feasibility of a policy framework to deploy this technology at large, private events in a more privacy protective way.

The goal of this paper is to explore the viability of the application of facial recognition technology to identify POIs at large, private events by examining the security benefits weighed against the costs to the event participants, the employing organization, and the necessary cybersecurity measures to ensure security and privacy.

Introduction

Facial recognition is a type of biometric identification technology. Biometrics are unique physical characteristics of an individual, such as fingerprints, retinas, and facial geometry that may be used for identification purposes.[1] In the case of facial recognition today, an individual's facial geometry is used for identification[2] or authentication.[3] The facial recognition industry is expected to grow to $7 billion by 2024 in the United States.[4] The technology continues to become more accurate and sophisticated and supports both public and private organizations in surveillance, identity verification or authentication, and data collection for marketing purposes. Indeed, facial recognition technology is already being utilized extensively in general and at large, private events and venues.[5] There has been, however, a strong call for more regulation of facial recognition software by privacy organizations[6] and even technology companies.[7] As facial recognition technology continues to advance and its use in security and surveillance increases, organizations must balance its use with the protection of individuals' personal data and privacy

[1] "Biometrics," US Department of Homeland Security, last modified July 13, 2020, accessed November 23 2020,https://www.dhs.gov/biometrics.

[2] Facial identification is the algorithmically returned potential matches of enrolled identities when compared to the captured image.

[3] Facial authentication is the algorithmic verification that an individual is who they purport to be (1:1).

[4] Nicole Martin, "The Major Concerns Around Facial Recognition Technology," *Forbes*, September 25, 2019, accessed February 24, 2021, https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/#437467e14fe3.

[5] Eric Chemi, "Sports Teams Are Using Facial Recognition To Learn More About Their Fan Bases," *CNBC*, April 21, 2018, accessed april 11, 2020, https://www.cnbc.com/2018/04/21/facial-recognition-helps-teams-and-advertisers-learn-about-fans.html.

[6] Dean Dechiario, "Privacy, Civil Rights Groups Plan Facial Recognition Offensive," *GovTech*, December 8, 2020, accessed January 19, 2021, https://www.govtech.com/security/Privacy-Civil-Rights-Groups-Plan-Facial-Recognition-Offensive.html.

[7] Dina Bass, "Microsoft Backs Facial Recognition Bill as Amazon Mulls Support," *Bloomberg*, February 7, 2019, accessed February 24, 2021, https://www.bloomberg.com/news/articles/2019-02-07/microsoft-backs-facial-recognition-bill-as-amazon-mulls-support.

by reviewing and considering new and evolving biometric privacy laws and personal data collection and protection measures.

This paper will explore the use of facial recognition technology for security and identification and how it may be applied at large, private events. For purposes of this paper, large, private events are defined as events hosted by private sector organizations that require purchase of tickets or registration and issuance of credentials for access, such as concerts, major sporting events, and industry conferences. This paper will also explore facial recognition technology benefits and limitations, and some real-world examples. It will analyze data protection and privacy implications of instituting such technology, biometric privacy laws, and models of deploying facial recognition at large, private events. It will make recommendations for achieving the two goals of using facial recognition for the purpose of identifying persons of interest (POIs) and protecting privacy and personal data. Facial recognition technology will continue to be developed with greater capabilities and accuracy.[8] If it is to be applied at large, private events, it is important for organizations to implement a consistent privacy protective policy.

Facial Recognition Technology Background

Facial recognition technology was first developed in the mid-1960s with funding from the U.S. government.[9] The technology has advanced rapidly since then and continues to do so today.[10]

[8] Robert Watts, "Facial Recognition as a Force for Good," *Biometric Technology Today,* no. 3, March 2019: 5-7, https://doi.org/10.1016/S0969-4765(19)30039-6.

[9] Jeremy Kahn, "Quicktake: Facial Recognition," *Bloomberg*, May 23, 2019, accessed February 24, 2021, (https://www.bloomberg.com/quicktake/facial-recognition.

[10] "Understanding Facial Recognition Systems," Partnership on AI, February 19, 2020, accessed on February 24. 2021, https://www.partnershiponai.org/wp-content/uploads/2020/02/Understanding-Facial-Recognition-Paper_final.pdf.

Facial recognition technology is software that uses an algorithm.[11] This algorithm identifies, measures, and analyzes the geometry of an individual's face, ultimately creating a template or unique code for comparison. When an image is introduced and the algorithm identifies that the image is in fact a facial image, it then measures facial attributes, or distinguishable landmarks such as the distance between the eyes, width of the nose, shape of the cheekbones, and length of the jawline.[12] A series of images are captured and subsequently translated into a template, or a set of numbers to represent the features on a subject's face.[13]

The algorithm has to be trained on a database of images, usually gathered through publicly available or specifically collected images, in order to perform facial recognition related tasks.[14] Without this training, facial recognition algorithms would be unable to perform adequately the functions of identifying and measuring facial attributes. The quality and number of images in the training data are important elements that affect the match capability and potential algorithmic biases of the software. Algorithmic bias is a conscious or subconscious preference by the developer of the algorithm for one group that affects the way data are collected, used, and developed for training, often leading to better outcomes or worse outcomes for one or more groups.[15] As an example, developers of facial recognition software may introduce bias by unintentionally focusing predominantly on one gender in training data which leads to an

[11] An algorithm is a set of instructions or rules created by a software developer

[12] Kevin Boonsor and Ryan Johnson, "How Facial Recognition Works," HowStuffWorks, accessed February 24, 2021, https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition1.htm.

[13] Ibid.

[14] "Understanding Facial Recognition Systems," Partnership on AI.

[15] Jake Silberg and James Manyika, "Notes from the AI Frontier: Tackling Bias in AI (and in Humans)," Mckinsey Global Institute, June 2019, accessed November 29, 2020, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Tackling%20bias%20in%20artificial%20intelligence%20and%20in%20humans/MGI-Tackling-bias-in-AI-June-2019.pdf.

algorithm producing more accurate matches for that specific gender. Researchers from MIT and Stanford University demonstrated gender bias in facial recognition algorithms in an experiment testing three algorithms. In particular, the algorithm error rates for determining gender of light-skinned men were never higher than 0.8 percent, whereas the error rates for darker-skinned women were 20 and sometimes 34 percent.[16] Algorithmic bias will be discussed further in the Challenges with Using Facial Recognition section below.

In a facial recognition system, known identified individuals and their images must be enrolled into the organization's facial recognition database. A facial recognition algorithm generally performs two functions with an acquired image: identification or authentication. This paper will focus specifically on the identification, and not authentication, properties of a facial recognition system that attempt to predict the identity of an individual, as that function is most relevant to identifying POIs among a crowd. Any newly acquired images are deconstructed to the predefined measurements or attributes established by the developer, converted into a template, and compared to a database of already collected, analyzed, and converted images (i.e., 1:N), ultimately producing a score on a potential match.[17] In other words, facial recognition involves comparing two digital templates, rather than two faces and in the context of identification, one template compared to many already stored templates.[18] The developer or operator of the software may set and adjust the match threshold, which is the minimum level the newly acquired image must achieve in order to be considered a potential match. Depending on that threshold, the

[16] Larry Hardesty, "Study Finds Gender and Skin-type Bias in Commercial Artificial-intelligence Systems," MIT, February 11, 2018, accessed January 19, 2021, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.
[17] Ibid.
[18] "Understanding Facial Recognition Systems," Partnership on AI.

software returns with a list of potential matches or templates that meet or exceed the identified threshold. The higher the threshold is, the more likely there will be fewer returned images. Conversely, the lower the threshold, the more returned images. It should also be noted that the higher the threshold, the higher potential for false negatives, or incorrectly indicating that the image/individual is not a potential match, and the lower a threshold, the higher potential for false positives, or incorrectly indicating that the image/individual is a potential match.

Facial recognition technology has become more prevalent within society today.[19] With the advent of better network and computer processing components, like graphics processing units, artificial intelligence and machine learning, facial recognition software has the capability to continue to evolve in accuracy and increase its potential value. According to the Federal Trade Commission, a group of workshop panelists attending a Face Facts workshop identified several developments that have contributed to the increased accuracy in facial recognition systems. These developments include better quality digital cameras and lenses that produce improved digital images, from which biometric data can more easily be extracted. There is also technology capable of producing 3D images to help reconcile pose variations in different images.[20] While facial recognition technology continues to develop and improve, there are many benefits to using the technology now.

[19] Kahn, "Quicktake: Facial Recognition."

[20] "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies," Federal Trade Commission, October 2012, accessed December 22, 2020, https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

The accuracy of facial recognition algorithms has improved significantly over the past few years. According to a 2018 National Institute of Standards and Technology (NIST) report evaluating 127 algorithms from 39 developers, facial recognition software became 20 times better between 2014 and 2018.[21] In fact, the NIST team found that just 0.2 percent of searches failed in 2018, compared with 4 percent in 2014.[22] The NIST report included results for the effects of aging on faces, scalability to large databases, identification of twins, and even the use of poor quality images.

Additionally, the accuracy of facial recognition software has increased to the point that some of the most accurate algorithms scored higher than forensic facial examiners at facial identification accuracy.[23] In a 2017 study published in the Proceedings in the National Academy of Sciences of the United States of America (PNAS), facial recognition software outperformed most human subjects and capabilities.[24] The results showed a steady increase in algorithm accuracy from a level comparable with students in 2015 to a level comparable with forensic facial examiners in 2017.[25] When the best facial recognition algorithm was paired with a forensic examiner, accuracy was at its highest.[26] As this technology continues to develop and sample sizes continue to increase and be more inclusive, algorithms should become more accurate.

[21] "Face Recognition Software's Capabilities," National Institute of Standards and Technology, last updated December 6, 2018, accessed February 24, 2021, https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities

[22] Ibid.

[23] P. Jonathon Phillips, Amy N. Yates, Ying Hu, Carina A. Hahn, Eilidh Noyes, Kelsey Jackson,...Alice J. O'Toole, "Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms," Proceedings in the National Academy of Sciences of the United States of America, June 2018, accessed February 24, 2021, https://www.pnas.org/content/pnas/115/24/6171.full.pdf.

[24] Ibid.

[25] Ibid.

[26] Ibid.

Use of Facial Recognition to Identify Persons of Interest

Facial recognition technology deployed at large, private events provides an additional tool to help safety and security professionals detect persons of interest (POIs) who may be dangerous to the organization, its employees, or attendees. Most private organizations, in the interest of protecting their employees and property, maintain an index of POIs who have either threatened to harm, have harmed, or have an unhealthy obsession with the organization or its employees. The results of this potential behavior can manifest itself in a number of different ways. In an extreme example, in 2018, a suspect who was upset with YouTube went to the company's headquarters in San Bruno, California and shot and wounded three people before killing herself on the property.[27] Large, private events can be viewed as an extension of a company's presence. These events often publicize their locations and schedules of guest speakers while also inviting and incentivizing members of the public to purchase tickets and attend. In addition, event credentials often do not contain strong security features and can be easily traded among temporary workers and attendees. A facial recognition identification system at a large, private event adds an additional layer of security by more quickly and efficiently identifying possible POIs and notifying security personnel.

Large, private events can present a challenge for security personnel due to the high volume of people. In 2019, the average number of attendees at a National Football League game was

[27] Holly Yan and Faith Karimi, "YouTube Shooter Visited Gun Range Before Attacking Strangers, Police Say," *CNN*, April 5, 2018, accessed February 24, 2021, https://www.cnn.com/2018/04/04/us/youtube-hq-shooting/index.html.

66,479.[28] Large corporate events may see similar numbers. Dreamforce, an annual Salesforce conference that takes place over four days, claimed 171,000 registered attendees in 2019.[29] Private companies may seek to and already utilize facial recognition to enhance safety and security capabilities at large, private events, that include industry conferences, conventions, concerts, or professional sporting events. For example, in 2001, facial recognition software was implemented at Super Bowl XXXV, scanning attendees as they entered the stadium, comparing their images to a wanted criminal database.[30] Similarly, in 2018, facial recognition technology was used at a U.S. concert to search for stalkers.[31]

The integration of facial recognition technology in support of security efforts offers a greater ability to process large volumes of data, leading to more specificity in investigative review, and essentially making the efforts more efficient.[32] Being able to search for or have targeted leads of known POIs makes more optimal use of security personnel and time. For example, if a facial recognition system alerts to a possible known POI, security personnel can monitor the POI's movements while directing additional response elements to a precise location for verification. The alternative would be a visual and manual search by security personnel for an individual or

[28] Christina Gough, "Average Per Game Attendance of Major US Sports Leagues 2019," *Statista*, July 14, 2020, accessed September 12, 2020, https://www.statista.com/statistics/207458/per-game-attendance-of-major-us-sports-leagues/.

[29] "Dreamforce 2019 in Review: Key Facts and Figures," *Salesforce.com*, December 3, 2019, accessed September 12, 2020, https://www.salesforce.com/company/news-press/stories/2019/12/Dreamforce-By-Numbers/.

[30] Declan McCullagh, "Call It Super Bowl Face Scan I," *Wired*, February 2, 2001, accessed January 19, 2021, https://www.wired.com/2001/02/call-it-super-bowl-face-scan-i/.

[31] Dareh Gregorian, "Facial Recognition Tech Used to Scan for Stalkers at Taylor Swift Show: Report," *NBC News*, December 13, 2018, accessed January 19, 2021, https://www.nbcnews.com/tech/tech-news/facial-recognition-tech-used-scan-stalkers-taylor-swift-show-report-n947581.

[32] James Byrne, and Gary Max, "Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact," Cahiers Police Studies, 2011: 32, https://www.ncjrs.gov/pdffiles1/nij/238011.pdf.

several known POIs within a crowd. Having this tool adds an additional layer of safety to the event because security personnel are more able to identify a potential threat to the organization and its attendees more quickly.

Challenges with Using Facial Recognition

Facial recognition software also has limitations. For example, developers design and train the underlying algorithm, which is heavily influenced by the range and quality of training data. Research indicates that algorithms perform better on the race that it was trained on. If an algorithm utilized predominantly caucasion images for training, it will be best at identifying caucasion faces.[33] Similarly, as evidenced by a NIST 2019 test on facial recognition, algorithms developed in China have lower false positive rates on East Asian faces.[34] In other words, the algorithm is being trained based on categorization and decisions by the developers, which influence the algorithm's accuracy. As such, organizations that deploy facial recognition technology should ensure the algorithm being used is trained on a robust, diverse, and quality dataset.[35]

Hardware and image quality also affect a facial recognition algorithm's ability to identify or match individuals. The image captured, the pose of the individual, lighting of the area and of the individual's face, and the presentation are all factors that influence accuracy.[36] Indeed, accuracy

[33] Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part3: Demographic Effects*, National Institute of Technology and Standards, NIST IR 8220, December 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[34] Ibid.

[35] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Line-up: Unregulated Police Face Recognition in America," Georgetown Law, Center on Privacy & Technology, October 18, 2016, accessed February 24, 2021, https://www.perpetuallineup.org/.

[36] Grother et al., "Face Recognition Vendor Test (FRVT) Part3: Demographic Effects."

decreases when there is no standard image for comparison or from an image acquired while a subject is moving or in an uncontrolled environment[37] which can often be the case at large events.

Due to recent advances in technology, specifically artificial intelligence and deep convolutional neural networks (DCNNs), algorithms have become quite tolerant of sub-standard images.[38] Neural networks are a subset of artificial intelligence where computer systems are designed and modeled after the human brain. DCNNs are a type of neural network that are able to process and learn specific features from massive amounts of data which can be utilized for classifying purposes, such as determining whether a facial image exists within a broader acquired sub-standard image.[39] Even while there continue to be advances in artificial intelligence and DCNNs, it may not yet be at an acceptable standard. For example, a 2018 audit released by the Department of Homeland Security's Office of Inspector General found that pilot programs to test facial recognition technology at nine airports had a combined match rate of 85 percent, below the agency's goal of a 97 to 100 percent match rate.[40]

[37] Kristine Hamann and Rachel Smith, "Facial Recognition Technology: Where Will It Take Us?" *American Bar Association*, Criminal Justice Spring 2019, v34 issue 1, accessed December 4, 2020, https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/.

[38] Grother et al., "Face Recognition Vendor Test (FRVT) Part3: Demographic Effects."

[39] Rafael C. Gonzalez, *Deep Convolutional Neural Networks*, Institute of Electrical and Electronics Engineers, November 2018, accessed November 29, 2020, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8496892.

[40] Hugo Martin, "Delta Air Lines Will Use Facial Recognition Cameras at LAX Boarding Gates," *Los Angeles Times*, Sept. 6, 2019, accessed February 24, 2021, https://www.latimes.com/business/story/2019-09-05/delta-air-lines-will-use-facial-recognition-cameras-at-lax-boarding-gates.

Further limitations also include hacks such as disguises when facial recognition technologies are known to be in place. Systems must be capable and trained to target specific facial landmarks that may not be as easily disguised. Even then, there are limitations with make-up, facial coverings, facial hair, other facial obstructions, and potentially distortions of the face (e.g, smiling, frowning). As an example, due to the COVID-19 pandemic, people have been wearing face coverings. Wearing a face covering limits the number of measurements a facial recognition algorithm can complete when building a template. In March 2020, NIST conducted a preliminary study testing commercial facial recognition algorithms in their ability to match images with digitally applied face masks to photos of the same individual without a face mask. The study noted that some algorithms had substantially higher error rates of 5 to 50 percent while others could not extract a face's features well enough to even make a comparison.[41] However, in December 2020, NIST again released a report noting that facial recognition algorithms submitted for similar masked faces testing following the arrival of the COVID-19 pandemic had decreased error rates, by a factor of 10, when compared to pre-pandemic algorithms.[42] While there was marked improvement in submitted facial recognition algorithms, it was noted that the algorithms were making error rates between 2.4 and 5 percent, comparable to where the technology was in 2017 on non-masked photos.[43] These results indicate that there remains much more work to be done to improve not only accuracy, but how facial recognition algorithms contend with disguises or spoofing attacks.

[41] "NIST Launches Studies into Masks' Effect on Face Recognition Software," *National Institute of Standards and Technology*, July 27, 2020, accessed December 22, 2020, https://www.nist.gov/news-events/news/2020/07/nist-launches-studies-masks-effect-face-recognition-software.
[42] "Face Recognition Software Shows Improvement in Recognizing Masked Faces," *National Institute of Standards and Technology*, December 1, 2020, accessed December 22, 2020, https://www.nist.gov/news-events/news/2020/12/face-recognition-software-shows-improvement-recognizing-masked-faces.
[43] Ibid.

Perhaps one of the greatest limitations on utilizing facial recognition technology for identification is a lack of trust and social acceptance of a tool often associated with surveillance. It is an important point to acknowledge because organizations in many industries and municipalities, in an effort to continue to promote and increase a level of transparency, trust, and maintain consumers' or residents' privacy, are electing not to implement facial recognition technology in its security programs. San Francisco was the first city to declare a ban on the use of facial recognition technology by city agencies.[44] Somerville, Massachusetts and Oakland, California did the same soon after.[45] Similarly, some companies that develop, market, and sell facial recognition software to law enforcement agencies, such as Clearview AI, are being sued by privacy advocates and civil liberties organizations, such as the American Civil Liberties Union (ACLU), for violations of privacy rights.[46] The ACLU, in a complaint, noted that Clearview AI is collecting and using Illinois residents' biometric identifiers without consent, which is required by the state's Biometric Information Privacy Act (BIPA).[47] Regardless of the outcome, it is important for a company to recognize that adopting facial recognition technology for security and identification purposes poses significant social, regulatory, and privacy challenges.

[44] Kate Conger, Richard Fausset, and Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," *New York Times*, May 14, 2019, accessed February 24, 2021, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

[45] Rachel Metz, "Beyond San Francisco, More Cities Are Saying No To Facial Recognition," *CNN*, July 17, 2019, accessed December 18, 2020, https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.

[46] Clare Duffy, "The ACLU Sues Clearview AI, Calling the Tool an 'Unprecedented Violation' of Privacy Rights," *CNN*, May 29, 2020, accessed February 24, 2021, https://www.cnn.com/2020/05/28/tech/clearview-ai-aclu-lawsuit/index.html.

[47] Ibid.

Most recently, several larger technology companies that develop facial recognition technology for identification purposes have declared a moratorium on selling it to police agencies due primarily to social concerns of widespread surveillance, encroachment on privacy, and the potential to misidentify subjects, increasing the risk of racial discrimination.[48] Amazon stated that its moratorium will last one year. Microsoft announced that it will wait until the U.S. Congress takes action to enact legislation on facial recognition technology.[49] Microsoft has long called for national regulation on facial recognition technology. Its argument is rooted in the basic human right to privacy and based on the principles of transparency, non-discrimination, notice, consent, and lawfulness.[50] Moreover, Microsoft incorporates an internal review process for any customer seeking to employ its facial recognition technology at scale.[51] These large technology companies, however, are not the only producers of facial recognition software that offer solutions to law enforcement agencies or private enterprises. In fact, these companies are not the primary vendors nor significant players in this market.[52] Indeed, there are over 80 vendors around the world offering facial recognition services and capabilities.[53] Furthermore, nearly half of all American adults are in a police facial recognition database, in part because of agreements that provide access to repositories of drivers license photos.[54] In comparison, particularly in the case of a private company, Clearview AI claimed to have built a database composed of three billion

[48] Brian Fung, “Tech Companies Push For Nationwide Facial Recognition Law. Now Comes the Hard Part,” *CNN*, June 13, 2020, accessed February 24, 2021, https://www.cnn.com/2020/06/13/tech/facial-recognition-policy/index.html.

[49] Ibid.

[50] Mary Jo Foley, “Microsoft Reiterates It Won't Sell Facial-recognition Tech to Police Until Federal Regulation Passed,” ZDNet, June 11, 2020, accessed February 24, 2021, https://www.zdnet.com/article/microsoft-reiterates-it-wont-sell-facial-recognition-tech-to-police-until-federal-regulation-passed.

[51] Ibid.

[52] Julia Horowitz, “Tech Companies Are Still Helping Police Scan Your Face,” *CNN*, July 2, 2020, accessed February 24, 2021, https://edition.cnn.com/2020/07/03/tech/facial-recognition-police/index.html.

[53] Ibid.

[54] Ibid.

scraped images from public sources,[55] which eventually led to cease-and-desist letters from large technology companies.[56]

There are significant challenges and several limitations that should be understood and considered when applying facial recognition technology at large, private events. Organizations need to weigh the security benefits derived from this additional tool amidst the social concerns of a surveillance state, misuse of technology and data, intrusion on privacy, and data protection.

Biometric Privacy Laws

In the U.S. there is no federal law regulating the collection and use of biometric data. However, there are a number of states that have passed biometric privacy laws, including Arkansas, California, Illinois, New York, Texas, and Washington. Although many states have not enacted biometric data laws, it is quickly becoming more of a concern for lawmakers.[57] In August of 2020, the National Biometric Information Privacy Act of 2020 was introduced in the U.S. Senate.[58] Although the bill has not been acted upon, it remains critical for an organization to understand how existing biometric privacy laws affect its ability to collect and process biometric data for facial recognition systems.

[55] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *New York Times*, February 10, 2020, accessed February 24, 2021, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[56] Horowitz, "Tech companies are still helping police scan your face."

[57] Natalie A. Prescott, "The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020," *National Law Review*, January 15, 2020, accessed December 18, 2020, https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

[58] Molly Arranz, "A National Biometric Privacy Law? Laws Protecting 'Biometric' Identifiers Continue To Cut A Blazing Trail," JDSUPRA, August 19. 2020, accessed December 5, 2020, https://www.jdsupra.com/legalnews/a-national-biometric-privacy-law-laws-80763/#:~:text=This%20month%2C%20federal%20legislation%20aimed,introduced%20in%20the%20U.S.%20Senate.&text=Specifically%2C%20it%20would%20prohibit%20private,consumers'%20or%20employees'%20consent.

A few examples of U.S. state laws that regulate the collection and processing of biometric data are the California Consumer Protection Act (CCPA) and the Illinois Biometric Information Privacy Act (BIPA). Additionally, the European Union (EU) General Data Protection Regulation (GDPR) is an example of regional data regulation. The GDPR is worth noting as it embodies privacy protective measures in data collection and processing for an entire regional population and may be reasonably used as a model for larger national scale privacy laws.

The CCPA governs the collection and use of biometric data of California residents and is applicable to companies that have over $25 million in annual revenue, or collect personal information on 50,000 people or devices, or receive more than 50 percent of their annual revenue from the sale of personal information. The CCPA requires that businesses that meet these criteria, no matter their location, provide California residents with the ability to understand, opt-out, delete, modify, or port any personal, or biometric, data the business has collected, even while CA residents are temporarily out of state.[59] If an organization collects and processes biometric data at an event hosted in California or with California residents in attendance, the CCPA applies. Therefore, as a practical matter, an organization should seek to comply with CCPA standards, since it can still be held accountable while operating out of state with California residents in attendance.

[59] California Consumer Privacy Act of 2018, Cal. Civ. tit. 1.81.5 (2018), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

Similarly, BIPA requires that private entities, defined as any individual, partnership, corporation, limited liability company, association, or other group, must, in order to possess biometric data have a written policy, available to the public, establishing a retention schedule; inform the subject, or their legal representative, in writing that biometric information is being collected; inform the subject, in writing the purpose for collection and length of retention; and receive a written release executed by the subject of the biometric identifier.[60] Organizations found not in compliance are subject to penalties; $1,000 for each negligent violation or $5,000 for each willful or reckless violation. The law also allows a private right of action, affording individuals and organizations the ability to bring action against the organization in question. Moreover, it does not require that a person demonstrate actual damage from having biometric data collected and processed to bring an action. Instead the act of violating BIPA is enough.[61]

Several lawsuits have been filed since BIPA was enacted in 2008. An example of potential monetary penalties associated with violating BIPA can be seen in Peatry v. Bimbo Bakeries USA, Inc. In brief, the plaintiff sued her employer for failure to obtain informed, written consent before obtaining biometric information and argued that each scan of her fingerprint every time she and 300 other employees clocked in and out of work accounted for a unique violation, potentially amounting to more than $5 million in damages.[62] The case is still on-going, with the

[60] Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14 (2008), accessed October 25, 2020, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[61] Prescott, "The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020."

[62] Michael D. Hayes, Robert J. Tomaso, and Anne M. Mayette, "Overview of Recent Decisions Interpreting the Illinois Biometric Information Privacy Act," *Husch Blackwell*, October 15, 2019, accessed January 19, 2021, https://www.huschblackwell.com/newsandinsights/overview-of-recent-decisions-interpreting-the-illinois-biometric-information-privacy-act#:~:text=Recent%20decisions%20have%20held%20that,are%20subject%20to%20BIPA%20mandates.&text=Union%20employees%20subject%20to%20a,or%20before%20an%20administrative%20board.

Court granting in part and denying in part Bimbo's request to dismiss[63], allowing Peatry to move forward with claims prior to the enactment of collective bargaining agreements between employees and Bimbo Bakeries. Comparatively, the number of attendees at a large, private event can easily surpass the number of plaintiffs in the Peatry case. In instances where organizations are found to be non-compliant, under a broad interpretation of each violation, damages may be exceedingly high. Organizations, then, should not apply facial recognition at large, private events in Illinois as the legal risk is heightened.

The GDPR also provides regulation on any collection, processing, and retention of the personal data of EU residents. Article 9 - Processing of special categories of personal data, notes that biometric data for the purpose of identifying a person are considered a special category of personal data and are generally prohibited from processing, with few exceptions that include explicit consent, protection of vital interests of a natural person, or processing of personal data that are manifestly made public by the subject.[64]

Understanding how these laws and exceptions apply can help develop a more privacy protective facial recognition model. For example, anonymization, as defined by the GDPR as personal data rendered to be no longer identifiable, causes the use case to be out of scope of the regulation.[65] Similarly, the CCPA, in section 1798.105 (d) (2), notes that a business need not comply with

[63] Peatry v. Bimbo Bakeries USA, Inc., No. 19 C 2942, (N.D. Ill. E. Div. 2020), https://www.leagle.com/decision/infdco20200226f32.

[64] EU Regulation 2016/679, General Data Protection Regulation, art. 9, 2016 O.J. (L 119/1), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679#d1e2051-1-1.

[65] EU Regulation 2016/679, General Data Protection Regulation, rec. 26, 2016 O.J. (L 119/1), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#d1e40-1-1.

requests to delete personal information, if it is necessary to detect security incidents or protect against malicious or illegal activity.[66] Thus, using a facial recognition system to search for POIs only, while anonymizing and deleting data collected from all other attendees, is a more proportionate, privacy protective, and viable model than requiring all attendees to be enrolled into a facial recognition database. Importantly though, while this model may be feasible under privacy laws such as the CCPA and the GDPR, it may not be under BIPA, since BIPA requires consent from any individual where biometric data are being collected and processed, including the POI.

While it is clear that organizations must follow any applicable state laws when employing facial recognition technology, it would be beneficial and prudent to model a program after some of the more prominent and restrictive biometric privacy and data regulation laws such as the CCPA, BIPA, and the GDPR. As a best practice, organizations should implement these types of standards at any large, private event where it may be deploying facial recognition technology, even in instances where there may not be applicable biometric privacy laws.

Case Studies of Identifying Persons of Interest with Facial Recognition

The following two examples describe real-world cases of using facial recognition to identify POIs. The first case study describes a model in which a company broadly uses continuous monitoring for authentication of employees and identification of POIs in a large campus setting. While the model is feasible to adapt to large, private events, it is also a higher-risk approach that

[66] California Consumer Privacy Act of 2018, Cal. Civ. tit. 1.81.5 (2018), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

reduces privacy and increases the potential of misidentification. The second case study provides a more proportionate approach that considers privacy protective measures and transparency when using facial recognition. Although in the second case the technology is employed by a police agency, analysis may be drawn and applied to private sector organizations and large, private events.

In March 2020, Intel implemented facial recognition technology on its campuses in Oregon.[67] It was noted that one of the primary purposes was to identify trespassers. The company, in an internal message board, indicated that it was particularly interested in identifying whether 200 individuals, deemed as especially serious threats or high-risk individuals, were on its property.[68] This task was challenging due to the number of offices within the same campus and a significant employee population. On its website, Intel publishes information on its facial recognition program. It states that the technology provides likely matches from live security camera footage with previously stored records,[69] indicating that the organization is using a constant monitoring model in which every facial image captured by a security camera is being collected and processed. The company also states that it collects badge photos of current and former employees, contingent workers, and privileged visitors, as well as images and video captured from security and safety incidents. The data collected are shared among its internal teams, namely security and human resources, and are used for safety and security purposes, which

[67] Mike Rogoway, "Major Tech Company Using Facial Recognition to ID Workers," *Government Technology*, March 11, 2020, accessed December 18, 2020, https://www.govtech.com/public-safety/Major-Tech-Company-Using-Facial-Recognition-to-ID-Workers.html.

[68] Ibid.

[69] "Facial Recognition Privacy Notice," Intel, last revised July 7, 2020, accessed December 18, 2020, https://www.intel.com/content/www/us/en/privacy/fr-privacy-notice.html.

include restricting access, investigations, and identification or location of individuals during emergencies.[70] Intel notes that it retains the templates of enrolled images for 10 years after an employee leaves under normal conditions, 30 years for individuals who are denied access to Intel facilities, and 31 days for any temporary templates created from live or recorded video footage.[71] The website also indicates that the data collected are secured and only accessible by authorized personnel with valid reasons to access the data.

Intel's facial recognition approach through real-time video surveillance or constant monitoring is complex and higher-risk.[72] The model is not recommended to be applied to a large, private event for a few reasons. First, it lacks privacy protective measures. Intel's model does not employ data minimization practices, instead requiring the enrollment of all employee, visitor, and POI biometric data.[73] Additionally, employee and visitor images would be constantly collected via video surveillance cameras and processed by the facial recognition algorithm. The task of enrolling and managing such an enormous amount of personal data of a large population is labor and time intensive. Moreover, a larger facial recognition database has a higher chance of containing individuals with similar features, potentially returning more possible matches that meet the prescribed threshold.[74] Second, it is unclear nor explicitly stated if written informed consent is received from visitors to its campus, which is a strongly recommended best practice. It is similarly uncertain what considerations the company took into account when discussing the

[70] Ibid.

[71] Ibid.

[72] Garvie et al., "The Perpetual Line-up: Unregulated Police Face Recognition in America."

[73] Ibid.

[74] Patrick J. Grother, George W. Quinn, and P. Jonathon Phillips, *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, National Institute of Standards and Technology, NIST Interagency Report 7709, August 2011, http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905968.

proportionality of how the perceived threats of the 200 high-risk individuals warrant a live video constant monitoring model with limited privacy measures. While Intel's use case is not recommended, other, more privacy protective models, exist.

In the second example, Cardiff University published a 2018 report on its evaluation of facial recognition technology deployment by the South Wales Police (SWP) at major events, which included the Champions League soccer competitions, festivals, and music concerts. Of particular relevance is the "locate" model where, similar to the Intel example, real-time video surveillance and constant monitoring was applied. However, in this instance, the acquired images were only compared to enrolled images of high-risk individuals or POIs and not an entire database of attendees.[75] The SWP also actively publicized its deployments of facial recognition technology. The technology was available for examination by members of the public if desired and was housed in a clearly marked and visible police van. Notably, the SWP also drew images exclusively from visible points on the exterior perimeter of the venue.[76] In other words, the facial recognition system was in a public area and not further integrated into surveillance camera systems within the venue of the events, preserving an element of privacy within the venue itself.

It is important to note that while the SWP has provided wider communications of its facial recognition program and intentions, the police agency does not obtain consent prior to collecting

[75] Bethan Davies, Martin Innes, and Andrew Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, Cardiff University: Universities' Police Science Institute, Crime and Security Research Institute, September 2018, https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5bdafb4403ce64828d6fbc04/1541077838619/AFR+Report+%5BDigital%5D.pdf.

[76] "Judicial Review Appeal FAQ," South Wales Police, accessed December 19, 2020, https://afr.south-wales.police.uk/#deploytitle.

and processing biometric information as it is a law enforcement agency afforded certain privileges. Conversely, private sector organizations, depending on applicable biometric privacy laws, would be required to obtain consent prior to collecting biometric information.

The study also notes that the SWP's application of facial recognition technology generally demonstrated improvement from past deployments. But, it also raised several privacy questions such as future uses, data storage, and retention.[77] In an effort to engage the community and increase transparency, however, the SWP maintains a public facing website with information about its facial recognition program that includes a privacy impact assessment, its purpose, type of data collected, processed, and retention schedules.[78] It also notes that the watchlists, or enrolled images within a facial recognition database, are limited and targeted towards individuals suspected of involvement in crimes.[79] The SWP practices data minimization by adapting the watchlist to the area of concern, denoting that the choice of deployment is not speculative, but instead there is good reason to believe that some of those on the watchlist may be at the locations where facial recognition is used.[80] As an example, due to a significant number of mobile phone thefts at major music events, the SWP utilized facial recognition technology at a music event held in Cardiff. Only individuals suspected of being part of an organized crime group specializing in mobile phone theft were enrolled into a specific facial recognition database created for that event.

[77] Davies et al., *An Evaluation of South Wales Police's Use of Automated Facial Recognition*.
[78] "Smarter Recognition Safer Community," South Wales Police, accessed December 19, 2020, https://afr.south-wales.police.uk/#deploytitle.
[79] Ibid.
[80] Ibid.

In terms of collection, processing, and retention, images of individuals who walk by the facial recognition system and are not a potential match are immediately and automatically deleted and unavailable to the system's operator or any police officer.[81] Specifically, the acquired data, or images, are anonymized and not usable or able to identify an individual. Images associated with a potential match are retained for 24 hours, but if no match is confirmed, they are deleted.[82] In addition, potential matches are only viewed and vetted by a limited cadre of trained facial recognition system operators.

The SWP's facial recognition program demonstrates a level of transparency and consideration for privacy that should be emulated by a private sector organization that operates facial recognition technology at large, private events. Notification of the presence of the technology prior to entering the event, publishing the type of data that are collected, how it is used, and if data are retained, are practices that better inform and provide transparency to attendees. Furthermore, the immediate and automatic deletion of images not deemed to be a potential match within the enrolled facial recognition database preserves individuals' privacy. Indeed, SWP's model and program attempts to enhance privacy by identifying ways to integrate privacy protective measures into a technology often associated with surveillance. Of course, a major difference is that a private sector organization should obtain consent to collecting biometric data from anyone that may be attending the event.

[81] Ibid.
[82] Ibid.

Putting facial recognition technology into action is not without its challenges. As illustrated by these two examples, there exist different strategies for activation, some with more privacy protective considerations and measures than others. Intel's model is broad in scope and perhaps more prone to a perception as a surveillance system, whereas SWP's use demonstrates a consideration for privacy, proportionality to threats, and social acceptability.

Recommended Standards for Using Facial Recognition at Large, Private Events to Identify Persons of Interest

An organization needs to consider carefully the risks and security benefits of utilizing facial recognition technology at large, private events to identify POIs. There is much efficiency to be gained from automation, as well as more accurate and steadfast capabilities over human vision.[83] Indeed, human security resources are susceptible to fatigue, distraction, and are just as prone to conscious or unconscious bias, unbeknownst to the employing organization. Using facial recognition, however, also presents many challenges. There are significant privacy consequences. It requires collection and processing of biometric data. In the course of data collection and processing, there must be security mechanisms in place to protect the data from unauthorized access or breaches. Prior to collecting and using data, notification and written consent should be obtained, and in some instances may be required due to biometric privacy laws. The process of establishing not only these standards, but also for potential legal challenges and data breaches are labor and time intensive. Moreover, the accuracy of facial recognition in identification, while generally better and more capable than a human counterpart, still varies in

[83] Phillips et al., "Face recognition accuracy of forensic examiners, super recognizers, and face recognition algorithms."

degrees of accuracy and some have been shown to contain algorithmic bias[84], increasing risk of misidentification.

With this in mind, the security benefits from using facial recognition at large, private events without a known significant and credible threat[85] do not outweigh the challenges associated with using the technology. In other words, facial recognition should not be in place for baseline security operations without a known significant and credible threat. If, however, an organization has heightened risk due to a known significant and credible threat, the added security capability of efficiently identifying the POI could certainly outweigh the aforementioned challenges. The organization, though, should take care to use facial recognition in a more privacy protective way, by instituting a comprehensive policy that contains the following administrative and technical controls to preserve privacy and protect personal data.

Administrative Measures

Privacy Impact Assessment

Organizations should conduct a privacy impact assessment (PIA). A PIA is an assessment to identify potential gaps in privacy, prior to commencing activities involving personal data, such as facial recognition. Specifically, an organization needs to identify the personal data it will be collecting, how they will be used, if they are to be retained and stored, and who would have access. The assessment demonstrates that the organization is making a conscious effort to

[84] Joy Buolamwini and Timnit Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” in *Proceedings of Machine Learning Research: Conference on Fairness, Accountability, and Transparency,* 2018 81: 1-15, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[85] Known significant and credible threats - a threat, physical action, or repeated conduct by a known person that causes harm and a reasonable person or organization to fear for his/her or its employees’ safety.

incorporate privacy protections throughout the development lifecycle of its facial recognition implementation.[86] As regulations increasingly call for organizations to be informative about data collection, a PIA helps collect needed information for compliance and provides greater transparency to attendees.

In 2019, the Government Accountability Office recommended the Department of Justice (DOJ) and Federal Bureau of Investigation take actions to ensure privacy when using facial recognition technology. It was suggested that the DOJ conduct a PIA, as required by the E-Government Act of 2002, to analyze how personal information is collected, stored, shared, and managed in federal systems, and system of record notices, which inform the public of the existence of the system and data collected.[87] Indeed, privacy assessments were conducted by the Customs and Border Protection Privacy Office for the Biometric Entry-Exit Program where privacy concerns were surfaced, addressed, documented, and eventually published to provide transparency on data collected and protection mechanisms.[88]

Proportionality

Organizations need also to examine the proportionality of using facial recognition at large, private events, weighing the potential security benefits against its effects on attendee privacy. For example, organizations could require, contractually, that entry into the large, private event

[86] "Face Recognition Technology - DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains," *Government Accountability Office*, June 2019, accessed November 1, 2020, https://www.gao.gov/assets/700/699489.pdf.

[87] Ibid.

[88] "Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot," *Department of Homeland Security Office of the Inspector General*, September 2020, OIG-20-71: 13, accessed October 25, 2020, https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

requires enrollment into a facial recognition database for purposes of identification or authentication. Facial recognition technology may be the only form of access control. This model requires that the attendees be provided information regarding the collection and handling of their biometric data and their explicit consent obtained. If consent is not provided, the individual is not permitted into the event. As noted by the Intel example, this model is feasible, but it is not recommended for use at large, private events. Moreover, it can be risky to rely solely on facial recognition for access control as technical issues relating to accuracy and throughput may present further challenges.

Alternatively, a model using facial recognition to identify POIs only can be explored. This instance would require a targeted enrolled facial recognition database of specific POIs and not attendees, limiting the number of enrolled images and minimizing the amount of data collected. It would also require real-time video surveillance and constant processing, but would include methods to make it more privacy protective, such as anonymizing technology and automatically deleting acquired images that are not potential matches within the enrolled facial recognition databases. These techniques preserve privacy, as the data are not exploited to identify an individual who is not within the enrolled database nor is it available to be used at a later time. Further, the facial recognition database would be employed exclusively for the event and not for any other purposes.

Notification and Consent

Clear warnings and information regarding facial recognition technology, its purpose, and the subsequent collection of biometric data, its use, and retention should be published and notification made to attendees and staff. Organizations should ensure that attendees understand and provide explicit and informed consent to the processing of their acquired images, in order to confirm they are not potential matches with POIs enrolled into the facial recognition database. It should be further explained that any acquired images or templates that are not a potential match with enrolled POI images or templates are anonymized and immediately and automatically deleted. Furthermore, the data collected should not be manipulated for any other purposes nor sold or shared with any third parties.

Enrolled Images and Database

The facial recognition database should incorporate data minimization practices by containing only enrolled images and templates of POIs. If the intention is to search for only a limited number of POIs, there is no further value to be derived from having a large database of other individuals or attendees.

Only POIs posing a significant and credible threat against the organization should be enrolled into the database. The POI should be known to have committed or threatened to commit a serious crime or harmful act against an organization's employees or property. This standard is analogous to law enforcement agencies requiring the assistance of facial recognition only in instances of serious felony level crimes such as homicide, robbery, and aggravated assault.[89] Limiting the database to targeted individuals prevents lower levels of accuracy. Unique or custom databases with enrolled images of specific POIs should be created for each event and

[89] Garvie et al., "The Perpetual Line-up: Unregulated Police Face Recognition in America."

subsequently deleted, along with any temporarily acquired images of potential matches that are not useful for investigative or prosecution purposes, after the event has concluded.

Written Policy

The operation of facial recognition technology should be guided by a written organizational policy, approved by the organization's senior leadership, and aligned with recognized privacy frameworks or principles developed by national organizations such as the NIST Privacy Framework[90], to bolster legitimacy. All policies must protect the constitutional rights of all persons and should expressly prohibit collection of images in violation of any existing regulation or rights afforded to individuals.[91] As an example, a policy should prohibit facial recognition from targeting or collecting information on individuals based solely on race, religion, or other attributes that may stifle protected free speech.[92] Moreover, policy should dictate limitations in data collection, use, and retention schedules. For example, a facial recognition system should not record video or retain acquired images unless there is an identified POI match. Only then should video or images be recorded and retained, but only for the necessary period. In essence, the written policy should provide operational guidelines based upon recognized best practices.

[90] "NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0," *National Institute of Standards and Technology*, January 16, 2020, accessed February 16, 2021, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

[91] "Interstate Photo System (IPS) Policy and Implementation Guide (Version 1.2)," *Criminal Justice Information Service Division, Federal Bureau of Investigation, U.S. Department of Justice*, September 2014.

[92] Garvie et al., "The Perpetual Line-up: Unregulated Police Face Recognition in America."

Technical Measures

Anonymization

In order to enable facial recognition technology in a more privacy protective way, organizations should implement anonymization controls. In essence, the acquired images of all individuals not associated with a potential match within the enrolled database should be anonymized so that they are not and will not be available for identification. Technologies are available that integrate with facial recognition systems to anonymize personal data by automatically blurring facial images captured on surveillance cameras or by altering the facial images, rendering them unable to identify an individual.[93] These technologies, coupled with the immediate and automatic deletion of data not associated with potential POI matches, offer organizations the ability to enhance privacy while using facial recognition technology. Organizations need to ensure that while the technology may still process personal data in order to identify POIs, it should do so in a way where images or data are only made available once a potential match has been identified.

Training Data and Match Thresholds

Organizations should also take due care to adopt facial recognition algorithms that are trained with diverse training datasets. A more diverse training dataset increases the accuracy of an algorithm.[94] Increased accuracy may decrease the number of returned potential matches or false positives. Similarly, a match threshold also influences the number of potential matches that are

[93] "Advanced Blurring Solution," Deidentification, accessed December 21, 2020, https://www.deidentification.co/advanced-facial-blurring/.

[94] Daniel Saez Trigueros, Li Meng, and Margaret Hartnett, "Generating Photo-Realistic Training Data to Improve Face Recognition Accuracy," *Arxiv*, October 2018, 11811.00112 v1, accessed December 5. 2020, https://arxiv.org/pdf/1811.00112.pdf.

returned by a facial recognition algorithm. Setting a high match threshold, coupled with a facial recognition algorithm trained on a more diverse dataset, increases privacy protection by limiting the number of potential matches, minimizing the amount of identifiable personal data processed.

Organizations should seek facial recognition algorithms that are trained using generative adversarial networks (GANs) and synthetic data. A GAN is composed of two neural networks, a generator and a discriminator, training each other through a feedback loop of data input and labeling. A generator generates synthetic data, in this case computer generated facial images that are not real but based on learnings from real images. A discriminator places a label of real or fake on the data produced by the generator. The generator continues to learn and produce better quality images based on each label prescribed by the discriminator, until the discriminator is no longer able to accurately label an image as fake or real. These high-quality images and their subsequent iterations may work to train facial recognition algorithms not only on spoofing or evasion techniques, but may also offer a deeper and wider range of training data without having to rely on facial images of real people.[95] Using synthetic biometric data reduces the instances of privacy related regulatory concerns.[96]

[95] Ibid.

[96] Andre Brasil Vieira Wyzykowski, Mauricio Pamplona Segundo, and Rubisley de Paula Lemes, "Level Three Synthetic Fingerprint Generation," *Arxiv,* August 2020, 2002.03809 v3, accessed December 5, 2020, https://arxiv.org/pdf/2002.03809.pdf.

Data Security

The level of encryption and data security is generally informed by the sensitivity and risk of the data to be secured.[97] Biometric data are considered sensitive personal data[98] under the GDPR and other legislation such as the CCPA and BIPA. Although within the United States there is no federal legislation categorizing biometric data as sensitive, it is generally perceived as being uniquely sensitive as it is a means to identification and cannot be changed.[99] Thus, facial recognition images and templates should be stored in a secure container that operates on its own dedicated network and system. The data should also be encrypted with strong encryption standards. Organizations should reference and implement security standards such as ISO/IEC 27001 - Information Security Management.

Organizations should also ensure strong security measures that protect biometric data and databases from unauthorized access or disclosure. Access to such data should be limited to a few trained personnel that require it only in furtherance of their duties and governed by a privileged access management system. The system should require an individual to login using a unique profile and password. The user should also be required to note the purpose, with specificity.

[97] EU Regulation 2016/679, General Data Protection Regulation, art. 32, 2016, OJ. (L 119/1), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679#d1e3383-1-1.

[98] Danny Ross, "Processing biometric data? Be careful, under the GDPR," *International Association of Privacy Professionals*, October 31, 2017, accessed November 6, 2020, https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/#:~:text=As%20mentioned%20above%2C%20in%20a,from%20specific%20technical%20processing%20relating.

[99] Arranz, "A National Biometric Privacy Law? Laws Protecting 'Biometric' Identifiers Continue To Cut A Blazing Trail."

An organization should assign a privacy and compliance specialist to monitor and audit any deployment of facial recognition at a large, private event. Samples from system logs and instances where the facial recognition system identified possible matches should be reviewed to ensure that operations conform with prescribed policy and regulation.

Conclusion

Facial recognition is a rapidly growing and evolving technology with several interesting applications, including use to identify POIs at large, private events. Although there is an advantage of greater efficiency, limitations, including algorithmic bias and privacy concerns, present serious challenges.

While facial recognition technology may provide an additional benefit and tool for security, its purpose should be weighed against the harm or threat to be mitigated. Indeed, the use of facial recognition technology should be in proportion to the threat or risk. Absent a known significant and credible threat against the organization or its employees, adoption of the technology for baseline security operations is not warranted. The risk to privacy and perception of constant surveillance is significant, as is the potential for misidentification. Lawsuits against companies that include it in its security operations continue to grow. Social acceptance of the technology, particularly when in service of security and identification purposes, is limited.

This does not signify that the technology is unacceptable at large, private events. On the contrary, it should be considered when there is a known or identified significant and credible threat against the organization or its employees. In such instances, a comprehensive policy including administrative and technical controls that support awareness and compliance with applicable biometric privacy laws, proportionality, transparency, notification, consent, and data minimization and security, should be adopted. As evidenced by the SWP, facial recognition technology can be employed in a more privacy protective way.