Face Recognition: A Struggle between Security, Convenience, Privacy, and Equity

A Sociotechnical Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Nikita Semichev

May 14, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Nikita Semichev

Sociotechnical advisor: Peter Norton, Department of Engineering and Society

Face Recognition: A Struggle between Security, Convenience, Privacy, and Equity

Facial recognition surveillance is proliferating worldwide (Feldstein, 2019). As components of access control, facial recognition systems can improve security. Such systems, however, can be subject to discriminatory biases and can compromise privacy. Because AI systems are subject to bias, they cannot be trusted unconditionally (Scharre et al., 2018). AI systems incorrectly match employees with darker skin more often than other groups (Cataleta, 2020). Social groups compete to draw the line between necessary security and invasions of privacy.

Companies and countries started to use facial recognition for surveillance and security (Ünver, 2018). As facial recognition capacities develop, authoritarian governments may abuse them at the expense of civil liberties (Sherman, 2019). Companies could be selling facial data of employees to the government. This could lead to increased surveillance and compromise the privacy of regular citizens. AI facial recognition technologies have become very accurate for specific datasets (Feldstein, 2019). Diverse datasets should be used to reduce racial bias in facial recognition algorithms (Cataleta, 2020). In a similar problem, parents monitoring online activity of teens, increased surveillance resulted in a change in behaviour and world perception (Youn, 2008). Privacy concerns can influence the behavior of employees and other participant groups.

Participants include security companies that serve building owners and tenants. Some sell facial recognition and fingerprint systems. FaceKey serves clients who want to “control access, shelter assets, prevent labor fraud and provide a safe workplace” (FaceKey, 2020).

But many privacy advocates oppose facial recognition, contending it is subject to discriminatory bias and invades privacy. They claim that facial recognition AI “misidentifies people of color, women, and children” and puts “vulnerable people at greater risk of systemic

abuse" (Fight for the Future, 2020). They are also concerned that collected information is "an easy target for identity thieves."

Some large tech vendors, including Microsoft, position themselves as responsible companies that take privacy seriously (Smith, 2018). Microsoft contends that governments and the tech sector "play a vital role" to ensure that facial recognition technology "creates societal benefits while curbing the risk of abuse." Some cities regulate surveillance systems. A New York City Council member stated that building owners' use of facial recognition technology "poses a serious threat to the rights of tenants," specifically, to "lower-income communities of color" (Lander, 2019).

In the U.S. since 2010, how have social groups competed to draw the line between necessary building security and invasive building security? Social groups have started using technologies and sophisticated algorithms that follow security protocols while also adhering to privacy concerns of the general public.

Review of Research

Politics play an important role in security issues and resolutions (Cavelty & Leese, 2018). Cavalry and Leese examine how politics impact security and surveillance policies. Their analysis brings together privacy and security using politicization, which will add a different perspective to the original research question. Rubinstein studied the effectiveness of "privacy by design," and how companies can reduce privacy concerns by following that principle (Rubinstein, 2011). If companies consider privacy issues before they implement necessary security measures, privacy concerns would be greatly reduced. Rubinstein also provides recommended practices for companies to follow when privacy can become a concern, which are useful for answering the

original research question. Moore studied security and surveillance conducted by the government and privacy concerns that come from it (Moore, 2011). Moore argues that some levels of privacy should come before any security regulations from the government. His research provides additional ideas and scope of information collected by the government and the dangers of disregarding privacy. Richardson observed that with the rise of facial recognition technologies, policymakers around the world have realized the potential risks of such technologies in regards to human rights (Richardson, 2021). Richardson states that although some legislation exists to prevent those risks, facial recognition is mostly unregulated. Crumpler and Lewis believe that facial recognition is not the problem itself, but rather the societal trends and technology-driven environment that makes it difficult to control (Crumpler & Lewis, 2021). They believe that national privacy legislation is necessary to guard against the risks of facial recognition. They state that in addition to regulation specific to facial recognition, general privacy laws regarding data collection and storage could be useful. However, they note that although regulation of facial recognition technology is necessary, overregulation may prevent innovation and should be avoided. Bannerman and Orasch conducted a survey in Canada on smart city privacy (Bannerman & Orasch, 2020). They found that privacy is a major concern and that many want more protection and control over personal data. They observed that Canadians were wary of private business storing and especially selling their data and wanted more control over their data. However, giving up some privacy for public benefit such as in traffic and city planning was generally more accepted. The researchers mentioned do not consider building security directly, but rather they analyze security, privacy and surveillance on a more general level. They indicate that, at a high level, security and privacy coexist. This fact has implications for building security.

Evolving Technological Advances

Innovation of new technologies and surveillance systems have urged private companies and government agencies to implement new security protocols within buildings to monitor and detect suspicious activity. AI facial recognition technologies have become sophisticated and provide accurate results. Many startups in recent years have been focused on AI and computer vision technologies, with many applications in security and surveillance. Sensory, an AI development company, started working on computer vision technologies to "improve speech recognition performance and accuracy," and stated that they are using AI to advance "efforts in biometrics and natural language" (Sensory, 2017). Speech recognition is also surveillance, and is related to face recognition. In 2017, IntelliVision announced "new high-accuracy AI/Deep learning-based face recognition and detection technology" that is highly accurate and achieved "accuracy benchmarks comparable to industry leaders" (IntelliVision, 2017). The accuracy benchmarks are tested on public datasets, which test for specific aspects of facial recognition. Megvii (Face++) and Vivo have launched several 3D facial recognition mobile applications, such as "3D secure payment and 3D plastic surgery," which will enable users to make mobile payments using facial recognition as their primary method of identity verification" (Face++, 2018). SenseTime, an AI startup, announced that "60 papers authored or co-authored by SenseTime were accepted to the biennial European Conference on Computer Vision," which "marks" a "significant milestone" in their "journey to discover new possibilities for computer vision" (SenseTime, 2020). Conferences such as this one also include many other papers that also contain breakthroughs in facial recognition technologies. Megvii reveals a new building access system MegPass, which uses "facial authentication technology" and has multiple features such as "fast authentication speed, high recognition accuracy in different lighting environments",

and “accurate recognition of people wearing accessories that partially cover their faces.” (Megvii, 2020). Other facial recognition and AI developers also focus on the aspects such as speed and accuracy of the system. A developer at Sentry has described the uses of drones and computer vision, such as traffic monitoring, parking lot management, and fire and smoke detection, some of which can be applicable to surveillance (Agarwal, 2020). Drones can be used for facial recognition specifically, which will create a new way to conduct surveillance. Sentry CEO believes that “AI is an essential element of any future security monitoring solution,” as the company announced partnership with Eagle Eye Networks to deliver “advanced AI-powered video analytics for physical security and public safety” (Sentry, 2020). In the past year as a result of the pandemic, several companies built solutions to mitigate the risks of COVID-19. Trueface created frictionless access control technology at air force bases to combat the spread of COVID-19 (Allen, 2020). As security access is necessary in some cases, companies work together with the government to develop solutions during the pandemic. IntelliVision announced face mask detection AI, that allows to detect a person wearing a mask in real-time (IntelliVision, 2020). They state that “face mask detection” is the “first of a number of products to be released” as ”part of a broader COVID-19 back-to-work solution.” Many other facial recognition and AI companies are working on new products and technological innovations that improve surveillance systems.

Privacy Concerns

With the increase of surveillance technologies, the general public has been cautious about preserving their privacy and wondering whether such means are necessary to provide security. Some groups do not trust private surveillance companies as they believe those companies could

be storing information and selling that data to other entities. Some activist groups argue against the use of modern AI surveillance technologies, due to racial bias in the nature of the software and limitations of privacy. Because of the racial bias, many are concerned about police forces using AI surveillance, as it puts specific groups at a higher risk of misidentification. One activist group believes that the “threats to privacy emerging from AI-augmented surveillance technologies must be addressed” (Live With AI, 2018). They agree that “surveillance can potentially improve law enforcement,” however, they are concerned to “tolerate reductions in privacy for the sake of greater security.” They also believe that “transparency is vital” and that “regulation and oversight of the use of surveillance technologies” should be conducted in a “manner transparent to the public”. Being transparent to the public would allow the surveillance technologies to gain more trust and reduce privacy concerns. A member of Human Right Watch states that “rights groups have raised alarm about” facial recognition surveillance use “to monitor public spaces and protests, to track and profile minorities, and to flag suspects in criminal investigations” (Toh, 2019). One of his concerns is that "technologies could single out racial and ethnic minorities and other marginalized populations.” He believes that “transparency is a prerequisite both for protecting individual rights and for assessing whether government practices are lawful, necessary and proportionate.” While some groups believe that AI surveillance provides some benefits and can be used properly under certain conditions, some groups do not support such surveillance at all. Ban Facial Recognition is one of anti facial recognition activist groups that believes that such technology “poses a threat to human society and basic liberty that far outweighs any potential benefits” (Fight for the Future, 2020). They also state that facial recognition technology “programmatically misidentifies people of color, women, and children.” They believe that this technology will be used to “control and oppress us.” Such groups believe

that facial recognition surveillance is a net negative and focus on privacy concerns and algorithmic bias. As the result of COVID-19 pandemic, “societal fears surrounding AI-powered surveillance have taken a back seat,” as the AI can be useful to combat the pandemic (Zola, 2020). He believes that technology such as AI surveillance is “is here to stay” and that “the benefits far outweigh its potential shortcomings." In contrast, another group states that the United States faces a “difficult challenge” in “balancing the development, use, and export of AI surveillance systems” while “not abandoning democratic norms” (Sahin, 2020). They believe that “pandemic has revealed the risks of AI surveillance tools” and “has the potential to further accelerate the use of technologies for social control.” Even the groups that are both partially concerned about privacy, disagree on whether the pandemic reduced or increased the concern about AI surveillance among the public.

Views of the Developers

The companies developing facial recognition technologies have issued statements regarding privacy concerns and data collection. Some companies support official regulations and promote ethical use of their software. Other companies focus on specific issues in their software such as algorithmic bias and discrimination. Kairos’s mission is to fix “misidentification of people based on ethnicity, gender, and age”, a problem which “plagues the facial recognition industry” (Moore, 2018). In law enforcement systems, the accuracy of face recognition “can mean the difference between disproportionate arrest rates and civil equality” (Brackeen, 2018). Improving the datasets that the facial recognition algorithms are trained on “will insure systems operate with more precision and reliability around ethnicity.” One of the common solutions mentioned to reduce algorithmic bias is to create training datasets that contain sufficient samples

from many different backgrounds, as most currently used datasets lack diversity. AnyVision does not “collect or share user data,” and tries to “ensure” that their “technology and products are used properly,” which takes into account algorithmic bias and racial discrimination (AnyVision, 2019). After the Senate introduced a bill that prohibited commercial companies using facial recognition tech from collecting or sharing user data, AnyVision stated that it is “in strong support of the bill.” (AnyVision, 2019). AnyVision states that facial recognition systems should be trained using datasets that are “diverse across race, ethnicity, age and gender” and should “perform with the highest level of accuracy in real-world conditions.” (Alexander, 2020). In addition, face recognition technology “must eliminate risk of data breach” that could be used to compromise someone’s identity. Sensory provides “embedded facial verification technology,” that authenticates users without “sending biometric data to the cloud,” and that Sensory is focused on developing AI that “improves the user experience but not at the expense of privacy” (Sensory, 2020). Trueface started using a new face recognition model, which reduces racial bias across all ethnicities (Behroozi, 2021). They are “committed to eliminating bias” in “face recognition models” and that they have a “responsibility to achieve parity of performance across all ethnicities and genders.” At Sentry, they believe that it is “possible to build ‘ethical’ AI” and that “the companies that build AI-based solutions should be held accountable” (Sentry, 2021). Also, “proper application of AI technology” can “lead to a safe and more prosperous world.” Kairos, a facial recognition AI company, brought back its founder, Brian Brackeen, an expert in algorithmic bias, to “address and eliminate racial bias from the technology” (Misoon, 2021). Many facial recognition AI development companies share similar ideas to protect the safety and privacy of the customers.

Regulations

Legislation systems have implemented laws that regulate companies and how much privacy they are allowed to sacrifice for building security. In addition, some private companies limit the amount of surveillance to respect the privacy of employees and the general public. As facial recognition technology is fairly recent, many bills are still pending to be reviewed. In 2019, senators introduced the Algorithmic Accountability Act, which "requires companies to study and fix flawed computer algorithms that result in inaccurate, unfair, biased or discriminatory decisions impacting Americans" (Cory Booker, 2019). The bill is endorsed by tech and civil rights groups, such as Data for Black Lives and the National Hispanic Media Coalition, which shows support from outside groups that are not primarily focused on facial recognition surveillance. The Commercial Facial Recognition Privacy Act of 2019 was introduced that would "prohibit certain entities from using facial recognition technology to identify or track an end user without obtaining the affirmative consent of the end user" (Blunt, 2019). The NIST issued a plan for "federal engagement in developing technical standards" in AI (NIST, 2019). The plan focuses on nine different areas for AI standards, one of which is trustworthiness, the standards for which include "guidance and requirements for accuracy, explainability, resiliency, safety, reliability, objectivity, and security." The California Consumer Privacy Act "defines biometric data, including facial recognition data, as personal information that is protected by the law" (Greenberg, 2020). This law gives consumers the "right to access their personal data and to request that it be deleted and not sold to third parties." It also obliges businesses to "protect the data." At least 22 states "added biometric data to the categories of personal information that must be reported if breached." In the next few years, it is likely to see more regulations in the sphere of AI surveillance.

Conclusion

As technology moves forward, it is inevitable that AI and facial recognition will become, if it is not already, a big part of our lives. The facial recognition industry is growing and many new applications can be used to improve the quality of life, however, there is certainly a concern of what will happen to our privacy. Even if algorithmic bias in the software is resolved, there are other issues such as data collection and potential security breaches that can compromise the privacy of many. Technological progress has skyrocketed in the past few decades and made it difficult to keep up with and regulate the evolving systems within a reasonable time frame. Facial recognition is not the only evolving technology that can potentially sacrifice privacy, there are many other outlets in modern technology where privacy or other similar violations can occur that currently do not have a definite solution. Another issue with such concerns is that different groups do not fully agree on what should be allowed and what regulations should be in place. For some, privacy might not matter in the slightest, while for others any amount of personal data about them can be a basis for a privacy violation. It is also difficult to interpret the statements made by technology companies about such issues at face value, as the companies run a business and the primary purpose of a business is to make profit. Although companies can make ethical decisions, it is difficult to tell whether they are telling the truth. Government regulations can also be problematic, as seen in China, and it's rather invasive surveillance systems. The United States is not an authoritarian state, but with the rise of modern technology and the trust that the public gives it, many freedoms that are currently enjoyed by many can be compromised. This case study could be improved by looking at other developed and developing countries and note similarities and differences in the approach taken by the government and the companies, and the

concern of the public. Studying other technologies and platforms such as social media can be useful to compare the difference in attitude with regards to privacy and safety. Many people around the world use smartphones, take photos and videos, and post to social media without much concern for their privacy but when technologies such as facial recognition surveillance are involved, it becomes much more controversial. Additional research could also examine how technology is introduced to the public and what effect it has on public opinion. Surveillance is seen as a negative, which could be one of the reasons why facial recognition technologies are controversial, since they are said to be directly involved with surveillance. The use of smartphones, however, although it can pose similar threats, doesn't have the same reputation. Going forward, several policy improvements could be made that would make facial recognition more acceptable and safe to use. The companies developing facial recognition software should be required to provide proof of using proper datasets for training and validate that there is no noticeable racial, age, or gender bias. In addition, it should be very clear where facial recognition takes place in public and private places. Any data that is stored about a person, should be available to the person and the companies that store that data must grant all deletion requests if someone wants to delete their own data. It is unclear what future innovations will bring, but respecting the privacy of the people and being transparent about the process is important to maintain trust in the government and commercial sectors.

References

Agarwal, R. (2020). Drones with Artificial Intelligence will soon become a powerful tool — a new perspective. https://medium.com/the-innovation/drones-with-artificial-intelligence-will-soon-become-a-powerful-tool-a-new-perspective-86f5e7e6f888

Alexander, T. R. (2020). AnyVision Offers 5 Indications for Fair, Ethical and Unbiased Use of Face Recognition Amidst Rising Public Debate.

https://www.anyvision.co/2021/01/08/anyvision-offers-5-indications-for-fair-ethical-and-unbiased-use-of-face-recognition-amidst-rising-public-debate

Allen, M. (2020). Combatting the Spread of COVID-19 with Frictionless Access Control at Air Force Bases. https://medium.com/trueface-ai/combatting-covid-with-frictionless-access-control-at-air-force-bases-697b19764cde

AnyVision (2019). Ethical and Responsible AI at AnyVision. https://www.anyvision.co/2019/08/06/ethical-and-responsible-ai-at-anyvision

AnyVision (2019). AnyVision Supports US Senate Bill on Facial Recognition. https://www.anyvision.co/2019/03/19/anyvision-supports-us-senate-bill-on-facial-recognition

Bannerman, S., & Orasch, A. (2020). Privacy and smart cities: A Canadian survey. *Canadian Journal of Urban Research*, 29(1), 17-38. JSTOR.

Behroozi, C. (2021). Trueface Reduces Bias Across all Ethnicities with Newest Face Recognition Model. https://medium.com/trueface-ai/trueface-reduces-bias-across-all-ethnicities-in-latest-face-recognition-model-fe5509eda298

Blunt, R. (2019). S.847 - Commercial Facial Recognition Privacy Act of 2019. https://www.congress.gov/bill/116th-congress/senate-bill/847/text

Brackeen. B. (2018). Face Off: Confronting Bias in Face Recognition AI. https://www.kairos.com/blog/face-off-confronting-bias-in-face-recognition-ai

Cataleta, M. (2020). Humane Artificial Intelligence: The Fragility of Human Rights Facing AI. *East-West Center*. JSTOR.

Cavelty, M., & Leese, M. (2018). Politicising Security at the Boundaries: Privacy in Surveillance and Cybersecurity. *European Review of International Studies*, 5(3), 49-69. JSTOR.

Cory Booker (2019). Booker, Wyden, Clarke Introduce Bill Requiring Companies To Target Bias In Corporate Algorithms. https://www.booker.senate.gov/news/press/booker-wyden-clarke-introduce-bill-requiring-companies-to-target-bias-in-corporate-algorithms

Crumpler, W. & Lewis, J. (2021). Questions about Facial Recognition. *Center for Strategic and International Studies (CSIS)*. JSTOR.

Face++ (2018). Megvii and Vivo unveil new 3D facial recognition applications at Mobile World

Congress Shanghai.
https://www.faceplusplus.com/blog/article/megvii-and-vivo-unveil-new-3d-facial-recognition/?cate=events

FaceKey (2020). Facial Recognition Access Control for biometric access control solutions.
https://www.facekey.com/solutions/face-or-fingerprint-recognition-systems/

Feldstein, S. (2019). The Global Expansion of AI Surveillance. *Carnegie Endowment for International Peace* (pp. 16-21, Rep.). JSTOR.

Fight for the Future (2020). Ban Facial Recognition.
https://www.banfacialrecognition.com/

Greenberg, P. (2020). Spotlight | Facial Recognition Gaining Measured Acceptance.
https://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measured-acceptance-magazine2020.aspx

IntelliVision (2017). IntelliVision Announces New High-Accuracy AI/Deep Learning-Based Face Recognition and Detection Technology for Smart Home and Smart Security.
https://www.intelli-vision.com/news/news3/

IntelliVision (2020). IntelliVision Announces Face Mask Detection AI Video Analytics.
https://www.intelli-vision.com/news/face-mask-detection/

Lander, B. (2019). New City Council legislation would protect tenants from facial recognition & "smart" key surveillance.
https://council.nyc.gov/brad-lander/2019/10/07/new-city-council-legislation-would-protect-tenants-from-facial-recognition-smart-key-surveillance/

Live With AI (2018). AI, Surveillance, And The Human Rights To Privacy.
http://livewithai.org/ai-surveillance-human-rights-privacy/

Megvii (2020). Megvii unveils new generation building access system MegPass.
https://en.megvii.com/news_detail/id/206

Misoon, V. (2021). Kairos Brings Back Founder Brian Brackeen To Continue Work Addressing Algorithmic Bias.
https://www.kairos.com/blog/addressing-algorithm-bias

Moore, A. (2011). Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability. *Public Affairs Quarterly*, 25(2), 141-156. JSTOR.

Moore, S. (2018). AI Frontiers: Kairos Untangles Face Recognition Bias.
https://www.kairos.com/blog/ai-frontiers-kairos-untangles-face-recognition-bias

NIST (2019). U.S. Leadership in AI: A Plan for Federal Engagement in Developing

Technical Standards and Related Tools. https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

Richardson, R. (2021). Facial Recognition in the Public Sector: The Policy Landscape. *German Marshall Fund of the United States*. JSTOR.

Rubinstein, I. (2011). Regulating Privacy by Design. *Berkeley Technology Law Journal*, 26(3), 1409-1456. JSTOR.

Sahin, K. (2020). The West, China, and AI surveillance. https://www.atlanticcouncil.org/blogs/geotech-cues/the-west-china-and-ai-surveillance/

Scharre et al. (2018). Artificial Intelligence: What Every Policymaker Needs to Know. *Center for a New American Security* (pp. 11-16, Rep.). JSTOR.

SenseTime (2020). SenseTime Explores New Computer Vision Possibilities with 60 Papers Accepted to ECCV 2020. https://www.sensetime.com/me-en/news-detail/55745?categoryId=21072

Sensory (2017). Staying Ahead with Advanced AI on Devices. https://www.sensory.com/staying-ahead-advanced-ai-devices

Sensory (2020). Facial recognition, verification, and identification; what they mean, the differences, and why it matters. https://www.sensory.com/facial-recognition-verification-and-identification-what-they-mean-the-differences-and-why-it-matters

Sentry (2020). Smart Sentry AI And Eagle Eye Networks Partner To Deliver Advanced AI-Powered Video Analytics For Physical Security And Public Safety. https://smartsentry.ai/2020/11/10/smart-sentry-ai-and-eagle-eye-networks-partner-to-deliver-advanced-ai-powered-video-analytics-for-physical-security-and-public-safety/

Sentry (2021). AI and Invasion of Privacy. https://smartsentry.ai/2021/04/08/ai-and-invasion-of-privacy/

Sherman, J. (2019). Essay: Reframing the U.S.-China AI “Arms Race”: Why This Framing is Not Only Wrong, But Dangerous for American Policymaking. *New America* (pp. 12-17, Rep.). JSTOR.

Smith, B. (2018). Facial recognition: It's time for action. https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

Toh, A. (2019). Rules for a New Surveillance Reality. https://www.hrw.org/news/2019/11/18/rules-new-surveillance-reality

Ünver, H. Akın. (2018). Politics of Digital Surveillance, National Security and Privacy. *Centre for Economics and Foreign Policy Studies*. JSTOR.

Youn, S. (2008). Parental Influence and Teens' Attitude toward Online Privacy Protection. *The Journal of Consumer Affairs*, 42(3), 362-388. JSTOR.

Zola, A. (2020). AI Surveillance in a Post-Pandemic World. https://securityboulevard.com/2020/06/ai-surveillance-in-a-post-pandemic-world/