Jaiden Atterbury, Xavier Lee, Nicholas Yu

Peter Gao

STAT 303

04 December 2022

Final Project Part Three: Final Report

**Introduction:**

Facial recognition technologies (FRTs) are a tool that have become more and more prominent over the years. They have slowly begun to play a role in the everyday life of an average person. From unlocking an iPhone to being used as evidence in a criminal justice case, FRTs are everywhere. FRTs are the set of digital tools that perform tasks on human faces through the use of images and/or videos. These tasks include, but are not limited to: face detection, face attribute classification/estimation, face verification, and face identification. Likely the most common example of an FRT is unlocking one’s phone. In this scenario, each time you attempt to unlock your screen, your phone’s camera will project and analyze the features of your face and match it to the stored data it’s familiar with to authenticate the user. Ideally, this technology works 100% of the time regardless of the subjects’ appearance. However FRTs are not flawless yet. There are numerous ethical concerns over racial biases, privacy implications, and the broad concept of liability. In this report, we’ll be going over why these ethical concerns have arisen and recommendations for what we think can be done to improve FRTs moving forward.

**Technical Details:**

In general, facial recognition works by identifying and measuring certain facial features in an input image, also known as a query image. Then, depending on which of the aforementioned uses was chosen, the machine outputs a decision on if a match or certain feature appeared in the query image. The query image can come in many different image data types. These image data types include: single images, video sequences, views from multiple cameras, and three-dimensional data. Due to the proprietary nature of the technologies themselves, most FRTs don’t function exactly the same. However, the majority of FRTs generally follow four broad steps when performing their duties, these steps are usually referred to as: capture and detection, enrollment, comparison, and matching decision.

To be used in an FRT, a face must be photographed or videographed so that it appears as one of the previously mentioned image data types. Once this query image is captured and a face is detected, the facial recognition system then analyzes this query image. It starts off by mapping and reading face geometry by identifying facial landmarks that are key to distinguishing a face from other objects. The system then converts this face data into a numerical format called a template or faceprint. The facial recognition technology typically looks at the following facial attributes when making a faceprint: distance between the eyes, distance from the forehead to the chin, distance between the nose and mouth, depth of the eye sockets, and shape of the cheekbones. Once the query image is transformed into a faceprint, there are two primary uses of this image data. The first of these uses is to build a gallery of people to be recognized. This process of recording visual information about an individual for the use in a gallery is called enrollment. The second major use of such photos is at the time of recognition, when the FRT is trying to identify or verify a person. The machine does this by comparing the query faceprint to the built gallery.

Once a faceprint has been extracted from a query image, the process of comparison then proceeds. The two main types of comparison that an FRT can perform are face verification, and face identification. In face verification, also known as one-to-one comparison, the goal is to confirm the identity of a certain query image by comparing the query faceprint to an existing faceprint of the expected individual. In this case the individual makes a claim about who they are and the task of the system is to verify this claim. The goal of face verification is to decide if two images show the same person (match) or two different people (mismatch). In face identification, also known as one-to-many comparison, the goal is to match an identity to given a face, without the expectation of who that person is. This process is done by comparing the query faceprint to

every individual faceprint in the set of faceprints in the gallery. When two faceprints are compared by a machine, a similarity score may be computed to represent the similarity of the two faceprints.

After the comparison has taken place the final step of the facial recognition process can take place, the matching decision. To decipher between match and mismatch, a certain score threshold must be set. Any scores above the threshold correspond to a match, and those below to a mismatch. Typically, one must make a compromise by setting a threshold which balances the number of false matches and false mismatches. During facial verification, when comparing a new query faceprint to an expected existing faceprint of the same individual, a similarity score is computed. Depending on the set threshold, the machine will either label the query image as a match or mismatch. During facial identification, when comparing a query faceprint to an entire gallery, one of three things can happen: no matches, one match, or multiple matches. In the event of multiple matches, an additional procedure will need to confirm the correct match, or decide that no correct matches are present. This job is usually left to a human to make the final decision.

**Ethical Concern #1: Racial Bias:**

While facial recognition technology does have many benefits, it does have its drawbacks. Unfortunately facial recognition technology has demonstrated a flaw that verifies faces of caucasian people with a higher precision than people of color. In his article *Report Finds Racial Bias in Facial Recognition Technology*, Jeff Stone writes, “According to the study, facial recognition systems are 5-10% less accurate when trying to identify blacks than when analyzing the facial images of white adults on the system.” This is especially concerning considering facial recognition systems are used in sectors of society such as law enforcement, travel, and even healthcare. Moreover, this bias is further compounding a discriminatory issue that has been negatively affecting people of color for decades. However, it is important to note that this doesn’t mean that the developers or the technology itself is racist. Rather, disparities may arise unintentionally as a result of designing the algorithm itself, lack of diversity in training data, and prioritizing certain facial features over others. The facial features that the algorithm analyzes tend to be distinguished more easily by fair skinned faces rather than darker toned faces. This includes features such as the shape of a person’s eyes, width of their nose, and the size of the person’s mouth or chin.

**Recommendation #1: Racial Bias:**

However there are new methods being developed attempting to eliminate the presence of racial bias in FRTs. Researchers are beginning to expand their datasets and stretch the domain of facial characteristics and racial features their technology is utilizing in its analysis. A recent report from the European Union News said that this research has led to a 1% improvement in reducing racial bias and has increased the accuracy of facial recognition across all ethnicities. While the disparity of 5-10% still hasn’t been closed, it’s important that we begin to address the issue and eliminate the bias in the technology we use. Eventually we should hope facial recognition technology becomes less dependent on race by focusing more on identifying features of a person’s face instead of relying on certain racial characteristics of the images as the algorithms currently do.

Another way to begin fixing racial bias in facial recognition technology is to ensure that the algorithms used by the technology are trained on a diverse dataset. This means using a dataset that includes a wide range of individuals from different racial and ethnic backgrounds, as well as a variety of ages and genders. By training the algorithms on a diverse dataset, we can help to ensure that the technology is able to recognize individuals from all backgrounds equally well. Next, another important step would be to regularly evaluate and test the accuracy of facial recognition technology. This can help to identify any potential biases and allow organizations to take steps to address them. For example, if a particular facial recognition algorithm is found to be less accurate for individuals from certain racial or ethnic backgrounds, steps can be taken to improve its performance for those groups.

Furthermore it’s important to have diversity and inclusion policies in place within companies that use facial recognition technology. This can help to ensure that the technology is being used in a fair and unbiased manner, and that individuals from all backgrounds are included and treated equally. To extend this point it’s crucial to involve individuals from diverse backgrounds in the development and implementation of facial recognition technology. By having a diverse team working on the technology, we can help to ensure that the technology is designed and used in a way that is fair and unbiased. Until these changes have been implemented and bias has been completely eliminated from facial recognition technology it’s important that law enforcement avoids using facial recognition technology altogether. It would be incredibly dangerous and ignorant to compound a discriminatory issue that has been affecting people for so many years. This can lead to individuals being unfairly targeted by law enforcement and even put at risk of wrongful arrest. By addressing the issue of racial bias, law enforcement agencies can help to ensure that the technology is used in a responsible and ethical manner.

**Ethical Concern #2: Privacy Concerns:**

One of the biggest existing ethical criticisms of FRTs are the broad privacy concerns that they bring to the individuals subject to their use. Privacy infringements have become one of the general public’s main concerns with FRTs, mainly due to a lack of transparency in how information is stored and managed. Furthermore, the most prevalent and scrutinized privacy implication of facial recognition technology is the use of the technology to identify individuals without their consent, this includes using applications such as real-time public surveillance or through databases that are not lawfully constructed. Without proper consent, FRTs take away the reassurance of being able to move and act freely without the fear of constantly being watched and surveilled. The use of databases that were constructed without the consent of the individuals in them is prevalent throughout the field of facial recognition, two of the most famous examples of this phenomenon are the MegaFace database, and the Clearview AI database.

The MegaFace database is one of, if not the most famous examples of the use of facial recognition without the informed consent of the individuals present in the database. MegaFace was a research project created in 2015 by two computer science professors at the University of Washington; Ira Kemelamcher-Schlizerman, Steve Seitz, and their graduate students. This database contained nearly 700,000 images scraped from the old social media platform Flickr. However, none of the people who appear in the MegaFace database were informed that their images would be used. In 2015 and 2016, the University of Washington held an event known as the “MegaFace challenge” in which the university promoted the use of the dataset to test up-incoming FRTs. Over these two years, it has been estimated that over 300 research groups worked with the database, with notable citations coming from Amazon, Mitsubishi Electric, and Phillips. It is important to note that despite the overall positive nature of the challenge, some companies such as SenseTime and NtechLab have been criticized for the way their algorithms have been implemented to perform unethical forms of surveillance.

The next, and one of the most recent examples of the use of facial recognition without the informed consent of the individuals present in the database, is the Clearview AI database. Clearview AI, which is self-described as the “world's largest facial network,” allows its customers to compare facial image data to over 10 billion images scraped from the internet. However, this database includes facial image data of a “substantial number” of UK citizens without these people's knowledge or consent. These images were scraped primarily from social media sites such as Facebook and Instagram. Furthermore, people who asked for their image data to be removed from the database often couldn’t proceed with their request due to Clearview asking them for additional personal information in order to meet their request.

**Recommendations #2: Privacy Concerns:**

Although individual privacy concerns such as the lack of informed consent are prevalent throughout the field of facial recognition, there are a few similar existing solutions that are being tried to combat this problem. These solutions primarily take the form of legislation, two examples of legislation used to combat the use of unethical collection of data are the Biometric Information Privacy Act and the General Data Protection Regulation (GDPR). Both of these acts/regulations seek to hold companies accountable for unethical data collection by imposing fines and sanctions on companies who violate the outlined laws.

By law, most Americans in databases such as the MegaFace database described in the previous section, don’t need to be asked for permission to be used in facial recognition databases. However, Illinois has the Biometric Information Privacy Act, a 2008 measure that imposes penalties for using Illinoisians biometric data such as faceprints without their consent. In the MegaFace database, there were thousands of photos from residents of Illinois. It is important to note that the Biometric Information Privacy Act doesn’t cover photos, instead they protect biometric data such as faceprints, fingerprints, iris scans, etc. However, due to the “MegaFace Challenge'' their biometrics were processed by hundreds of companies when used as test data for their FRTs. Due to this clear violation, those individuals whose biometric data were used without their permission are entitled to $1,000 per use, and $5,000 per “reckless” use. The legislation has turned out to be effective as over 200 class-action lawsuits claiming companies have illegally used individuals’ biometrics have been filed in Illinois since 2015, including a $35 billion dollar lawsuit against Facebook. Recently, technology companies have been very cautious in states with biometric laws.

The next existing remedy to the lack of informed consent in facial recognition is the GDPR, the self-proclaimed “toughest” privacy and security law in the world. Although the GDPR was passed by the EU, it imposes obligations on organizations anywhere, given that they illegally collected data on individuals from the EU. In response to violators, the GDPR levies harsh fines against those who violate the privacy and security standards drafted in the bill. Under the GDPR companies can only process data from subjects if the subject gave the company “specific, unambiguous consent” to process the data. In the aforementioned Clearview AI example, Clearview AI failed to comply with the higher data standards set by the GDPR. This misuse of data of individuals from the UK has led to them receiving a 17 million pound fine. The GDPR has been very effective in forcing companies to think strategically regarding the use of consumer data. Furthermore, the risk of incurring hefty fines has made companies take privacy and security more seriously.

Although these current forms of legislation have been very effective in combating the lack of informed consent in FRTs, due to the fact that as of the first quarter of 2022 only 7 states have biometric privacy laws based on that of Illinois, the legislation is not enough to fully combat this lack of consent in facial recognition. Furthermore, in states that don’t have biometric privacy laws Americans in facial recognition databases don’t need to be asked for permission to be included in said databases. Thus, in order to fully combat this lack of consent and clear violation of citizens privacy, we must create a task force that would draft an act very similar to that of the Biometric Privacy Act in Illinois, but make it federally effective. By doing this the act would impose certain obligations on companies/businesses in every state, including obtaining consent before any collection and use of biometric data, forcing these companies to explicitly state how the biometric data will be used and stored, and lastly making these companies employ reasonable security measures to ensure the safety of ethically obtained biometric information.

**Ethical Concern #3: Liability:**

Among the ethical issues of FRTs, the issue of liability has been slowly rising to the surface. The topic has not been popularized yet as technology and the concept of AI are still being adopted by society. However, as more and more industries are putting FRTs into practice, judges and society as a whole are starting to find the need for setting boundaries in these gray areas. For example, the healthcare industry has been carefully implementing FRTs in its hospitals and their accompanying systems. However, one growing concern of the general public is a scenario where FRT diagnostic software advances to a point where it far exceeds the role of assisting physicians and replaces them entirely. Furthermore, without human oversight this could lead to a case where the algorithmic decision-making tool could make the wrong decision, which could be lethal in extreme cases. It is in this scenario where the ethical and legal questions arise asking which party is liable. Is the hospital at fault since the event took place in the hospital? Perhaps the physician should’ve been on the site? Or is the software company to blame for failing to prevent a malfunction in the code? What if the patient entered the wrong information, but the FRT wasn’t trained for the unforeseen case, and, therefore, gave the wrong diagnosis? All of these encapsulate the concern of liability that is created by FRTs in high-stakes sectors such as healthcare.

One unpopular opinion about the use of FRTs that usually goes unnoticed by society and the media is that companies can also be the victims of liability disputes. For instance, Illinois has recently passed the aforementioned Biometric Information Privacy Act, also known as BIPA. Under this state law, private entities cannot collect or store facial template data without first notifying the user/consumer. After notification, the private entities must acquire written consent from the user and disclose any relevant information, such as the purpose and intended usage of the data collection. BIPA also contains a private right of action provision that binds companies to compensate for any statutory damages at a minimum of $1,000 and up to $5,000. The problem here lies in how the Illinois Supreme Court made it easier for the plaintiffs to win a false accusation. This problem is exemplified by the fact that plaintiffs can pursue BIPA claims even if they did not suffer from any actual damages. An exemplary case would be the court case of Rogers v. BNSF. In this case, the plaintiff alleged that BNSF collected biometric data from the workers to confirm identity and access its facilities, but did not disclose the reason for data collection and retention. BNSF argued that they shouldn’t be responsible for the decisions made by a third-party contractor, but the judge took the plaintiff’s side nonetheless. As a result, BNSF had to pay $5,000 to nearly 45,600 workers, paying a total of $228 million. Of course, there may have been certain details that weren’t made available to the public regarding the court case to say that BNSF was entirely the victim. Nevertheless, we still do not have enough laws outlining the lawful and ethical uses of FRTs and biometric data collection. Furthermore, the existing laws are not encompassing enough to rule fairness for both parties - the users and the company.

**Recommendation #3: Liability:**

To solve this problem of liability disputes, the government should introduce more FRT-specific regulations. It is important to note that FRTs are a complicated and delicate technology that requires close study by expert-level knowledge holders. Hence, it would be unavoidable to work with companies when setting a technology-specific regulation, especially one that is as new as FRTs. Furthermore, the regulations and legislation may still have loopholes at times and may not sufficiently cover all areas. Nevertheless, these regulations will serve as official statements from the government and thus will hold powers and act as guidelines for the public to follow. With more precedents and attention brought by the media, people will become more aware of the areas to develop on and more familiar with cases that are gray and ethically challenging. Due to the rise of public awareness that regulation will bring, this will eventually lead to more answers on what needs to be done in future regulations and laws. Slowly, society will be able to set firmer boundaries and allocate liabilities more fairly.

Additionally, for the boundaries to be effective at their intended purpose, companies should be strictly forced to abide by the stated laws. As a starting point, companies can follow the BIPA and other similar laws like the Washington Privacy Act (WPA). Even though the companies may have to carry more liabilities as mentioned previously, it is also true that in the past companies have been more free of liabilities, exploiting the blind spots in current laws and the general public’s lack of professional and technical knowledge surrounding business laws. Hence, a process of recalibration is needed to reset this balance. Moreover, for future regulation to be able to allocate liabilities more reasonably, the currently set laws must be followed faithfully.

**Connections:**

The ethical concerns discussed above are not unique to FRTs only. Racial biases, for instance, could be found in other algorithmic decision-making systems, such as Twitter’s saliency algorithm. In 2021, Twitter introduced a new algorithm that automatically cropped images for its users. The way the image was cropped was through the use of a saliency algorithm. This algorithm worked by analyzing the uploaded image to select what was deemed ‘important’ and would therefore be centered in the cropped frame. However, soon after the algorithm was published, users found that the algorithm was inherently racially biased. For instance, if a user were to upload the faces of Mitch McConnell and Barack Obama in the same image, Twitter’s algorithm would judge McConnell’s face to be more salient in comparison to Barack's. Later, when experts ran more tests to confirm the issue, they found out that the biases not only persisted amongst the different races but in gender as well. The test results showed that between men and women, pictures of women were 8% more likely to be marked salient in comparison to their counterparts. For white and black individuals, the former individuals were 4% more likely to be scored higher in general, and white women, compared to black women, were 7% more likely to receive higher scores from the algorithm.

A similar pattern of ethical concerns were raised in the use of hiring algorithms as well. Hiring algorithms use past data to deduce the best job candidates for the company using the algorithm. In other words, if the company has displayed biases in its past hiring decisions, then the algorithm is likely to perpetuate these biases when selecting future candidates. As an example, Amazon’s hiring algorithm was biased against women despite its developer team’s best efforts to mitigate these biases. These biases were the cause of the past ratio of the gender of the hired job candidates being predominantly male. As a result, the algorithm automatically ruled the screening process in favor of men. The algorithmic decision-making system gave a lower score to the resume that held any hints of the candidate being a female, such as using words like him, women, her, etc. As such, one can easily come across algorithmic biases in the most mundane settings in today's society.

Lensa is an exemplary case of how data can be collected without consent and without these same people knowing how their privacies are being invaded. The algorithm-driven automated software prints a portrait of any users if they were to upload an image of themselves. Users praised the application for its unique and creative drawing style, except that it wasn't original. It turns out, the algorithm searched through its database to select various artists' works and copy the styles without notifying or acquiring consent. The application's trick was debunked because the algorithm wasn't sophisticated enough to cover the artists' signatures. Lauryn Ipusm, a professional illustrator and the victim of Lensa, said that the problem lies in not paying what is due, which includes consent, compensation, and credit. Nevertheless, the app developers never addressed the issue of copyright in their tweets, and users continued to incorporate the application in their video content.

Unfortunately, new ethical concerns from algorithmic decision-making systems are raised every day despite the best of intentions from developers. That is because much of our data contains biases and malintentions, and the algorithms only do what they are best at, learning from the past. With that said, perhaps algorithms aren't about automating services for convenience, but more about reflecting our past decisions.

**Works Cited:**

“(740 ILCS 14/) Biometric Information Privacy Act.” *Illinois General Assembly*, <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>.

ACLU of Washington. “Automated Decision Making Systems Are Making Some of the Most Important Life Decisions for You, but You Might Not Even Know It.” *ACLU of Washington*, 21 Jan. 2022, <https://www.aclu-wa.org/story/automated-decision-making-systems-are-making-some-most-important-life-decisions-you-you-might>.

Au, Wagner James. “Lensa Scraping Artists' Work without Their Consent into Its ‘AI’ Images -- Even the Artists' Signatures!” *New World Notes*, 7 Dec. 2022, https://nwn.blogs.com/nwn/2022/12/lensa-ai-art-images-without-consent.html.

Bedoya, Alvaro M. “You Cannot Encrypt Your Face.” *The Atlantic*, Atlantic Media Company, 5 May 2017, <https://www.theatlantic.com/technology/archive/2017/05/you-cannot-encrypt-your-face/524073/>.

Buolamwini, Joy, et al. “Facial Recognition Technologies: A Primer.” *CIRCLS*, 29 May 2020, <https://circls.org/primers/facial-recognition-technologies-a-primer>.

Char DS, Shah NH, Magnus D. “Implementing machine learning in health care—addressing ethical challenges” *N Engl J Med.* 2018;378(11):981-983.

Chowdhury, Rumman. “Sharing Learnings about Our Image Cropping Algorithm.” *Twitter*, Twitter, 19 May 2021, https://blog.twitter.com/engineering/en\_us/topics/insights/2021/sharing-learnings-about-our-image-cropping-algorithm.

Davies, Rob. “US Facial Recognition Firm Faces £17m UK Fine for 'Serious Breaches'.” *The Guardian*, Guardian News and Media, 29 Nov. 2021, <https://www.theguardian.com/technology/2021/nov/29/us-facial-recognition-firm-faces-17m-uk-fine-for-serious-breaches-clearview-ai>.

DiRago, Molly S., et al. “A Fresh ‘Face’ of Privacy: 2022 Biometric Laws.” *Troutman Pepper*, 5 Apr. 2022, <https://www.troutman.com/insights/a-fresh-face-of-privacy-2022-biometric-laws.html#:~:text=Assembly%20Bill%20A27%3A%20Establishing%20the%20Biometric%20Privacy%20Act.&text=If%20passed%2C%20it%20would%20impose,measures%20to%20safeguard%20biometric%20information>.

Friedel, Laura, and Elizabeth Vandesteeg. “Jury Awards Plaintiffs $228 Million in Illinois Biometrics Class Action.” *JD Supra*, Levenfeld Pearlstein, LLC, 20 Oct. 2022, <https://www.jdsupra.com/legalnews/jury-awards-plaintiffs-228-million-in-3359726/>.

Gangarapu, Katam Raju. “Ethics of Facial Recognition: Key Issues and Solutions.” *Learn Hub*, 25 Jan. 2022, <https://learn.g2.com/ethics-of-facial-recognition>.

Hill, Kashmir, and Aaron Krolik. “How Photos of Your Kids Are Powering Surveillance Technology.” *The New York Times*, The New York Times, 11 Oct. 2019, <https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html>.

Jones, Anthony. “GDPR Three Years Later: What Impact Has It Made?” *I.S. Partners*, 16 Aug. 2022, <https://www.ispartnersllc.com/blog/gdpr-one-year-later-impact/#:~:text=countries%20and%20states.-,The%20Global%20Impact%20of%20GDPR,privacy%20and%20security%20more%20proactively>.

Lewis, James Andrew. “How Does Facial Recognition Work?” *Center for Strategic and International Studies*, 10 June 2021, <https://www.csis.org/analysis/how-does-facial-recognition-work>.

Liberties.EU. “7 Biggest Privacy Concerns Around Facial Recognition Technology.” *Liberties*, 25 Oct. 2022, <https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518>.

Martinez-Martin, Nicole. “What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?” *Journal of Ethics | American Medical Association*, American Medical Association, 1 Feb. 2019, <https://journalofethics.ama-assn.org/article/what-are-important-ethical-implications-using-facial-recognition-technology-health-care/2019-02>.

Oberly, David, et al. “Facial Recognition Technology: Minimizing Risk in the Face of Increasing Liability.” *Security Magazine RSS*, Security Magazine, 26 Feb. 2020, <https://www.securitymagazine.com/articles/91787-facial-recognition-technology-minimizing-risk-in-the-face-of-increasing-liability>.

“Reducing Racial Bias in Facial Recognition.” *Gale General Onefile*, 13 July 2020, <https://go-gale-com.offcampus.lib.washington.edu/ps/i.do?p=ITOF&u=wash_main&id=GALE%7CA629447107&v=2.1&it=r>.

“Researchers Flag up Facial Recognition Racial Bias.” *ScienceDirect*, 20 May 2016, <https://www-sciencedirect-com.offcampus.lib.washington.edu/science/article/abs/pii/S0969476516300790>.

Rosencrance, Linda. “Privacy and Security Issues Associated with Facial Recognition Software.” *TechRepublic*, 25 Aug. 2022, <https://www.techrepublic.com/article/privacy-and-security-issues-associated-with-facial-recognition-software/#:~:text=People%20who%20use%20facial%20recognition,technology%20are%20targets%20for%20hackers>.

Stone, Jeff. “Report Finds Racial Bias in Facial Recognition Technology.” *ProQuest*, 18 Oct. 2016, <https://www.proquest.com/docview/1829940128?accountid=14784&cid=CID:20221206170528367:934051&fromOL=true&parentSessionId=CovxMwrf6VZDN7wzCTIitq3niWdaXZIFJjzmLn5txY0%3D&parentSessionId=GKL50dW1tJIEXLu3OxKG6iXKyCiVzke0Wv%2BTS57DlSA%3D&pq-origsite=primo>.

Sullivan, Hannah R., and Scott J. Schweikart. “Are Current Tort Liability Doctrines Adequate for Addressing Injury Caused by Ai?” *Journal of Ethics | American Medical Association*, American Medical Association, 1 Feb. 2019, <https://journalofethics.ama-assn.org/article/are-current-tort-liability-doctrines-adequate-addressing-injury-caused-ai/2019-02>.

“What Is Computer Vision?” *Amazon*, Springer, 2015, <https://aws.amazon.com/computer-vision/>.

“What Is Facial Recognition?” *Amazon*, The University, <https://aws.amazon.com/what-is/facial-recognition/#:~:text=It%20works%20by%20identifying%20and,large%20collection%20of%20existing%20images>.

“What Is GDPR, the EU's New Data Protection Law?” *GDPR.eu*, 26 May 2022, <https://gdpr.eu/what-is-gdpr/>.