Tech for Humanity Case Studies

The Gaze of Others

No one can lie, no one can hide anything, when he looks directly into someone's eyes.
– Paulo Coelho

Reema was the first woman in her family to go to university. Her parents had immigrated as refugees from Afghanistan during the United States' War on Terror. Her father had been a translator for the U.S. Army and had fled one-year before the U.S withdrew its last soldiers from the country. Reema spoke English well and had excelled in her final two years of high school in the United States. She had arrived at the height of the Covid-19 pandemic and her first year had been online but by her senior year she had enjoyed going to school in Fairfax, Virginia. She learned quickly to adapt to American culture while keeping in touch with her cultural and religious roots from Afghanistan. In the summer of 2021, her father had taken her on a college tour of universities on the East Coast. At the dinner table each night her father and mother spoke to her about how she would have so many opportunities while attending university in the United States. Opportunities she never dreamed about while living in Afghanistan. By the spring of 2022 she had applied to and been accepted to several solid universities and had chosen to attend one of the large in-state universities. She planned to be a pre-med major with the hope of becoming a doctor and helping people. Discussions around the table also included conversations on how to adhere to Islamic traditions while also enjoying all the wonderful opportunities that university would open for her. Reema believed strongly in wearing a head covering called a hijab to serve as her Iman, a recognition of faith, and to ensure her modesty. Her parents and Imam (religious leader) had encouraged her to retain this article of faith as she transitioned to university life. They knew that it would be difficult for her, and she would stand out within liberal western universities. The hijab is typically worn in public.

Reema took a full load of courses at the university including introductory biology and others that set her on the path towards completing a pre-med degree. At the mid-point of the semester her professor for her introductory biology course assigned all the students a mid-term exam to be taken at home or in the dorm. Reema was not concerned about taking a test at home and had previously taken many tests and classes via computers while in high school during the Covid-19 pandemic. This time, however, was different. When Reema logged into the university's learning management system and clicked on the link to take the exam she was redirected to a page for online exams with a built-in anti-cheating software known as EyeThentic. EyeThentic requested she install a software plugin on her computer. She complied. EyeThentic then asked for permission to access her computer's web camera, microphone and the computer's infrared facial recognition system that was used to log her into to her computer. Increasingly wary with each request but not wanting to miss the deadline for when she had to take the online exam she complied. When EyeThentic was done asking for permissions to each of the aspects of her home computer system she was then asked to raise her laptop and show it in a 360-degree arc around her room. It asked her to show her desk. It also asked her to look at the camera and show her

face in a revolving circle. When it detected her hijab it asked her to remove the hijab so that it could complete its facial scan. At this point Reema was uncertain how to proceed. She had already given EyeThentic access to view her entire computer, scanned her room, and her face and now she was being asked to violate religious tradition so that she could take a test. She quickly texted her mother and father who told her to reach out to the professor.

Reema emailed the professor, and he responded in 15 minutes and said that he understood, but that unfortunately this was the only option for taking the test and that if she wanted to complete this test, she needed to comply with EyeThentic. What he didn't mention was that during the pandemic he had experienced a steady rise in academic dishonesty cases involving students and he felt it was his ethical duty to ensure that students didn't cheat on tests, particularly students who were on a pre-med track. Frustrated, Reema complied. She felt violated by this anti-cheating software but reasoned that it wasn't truly a violation of her religious commitment as it was only an AI that was viewing her.

Reema took the exam. She did her best to stay focused while taking the test, keeping her eyes on the screen. But as she worked through the exam her gaze inadvertently started wandering upward as she pondered her sacrificing her dignity for the purpose of taking a test. EyeThentic began issuing automated warnings to her notifying her that her gaze was wandering. She completed her test, and it was automatically sent to her professor. What Reema didn't know was that because her gaze had wandered during her test the AI sent a video recording of her taking the test both to the AI engineers at EyeThentic and a copy to her professor. Moreover, because the AI had been primarily trained on white faces its interpretations of Reema's facial movements and gaze has become increasingly negative. It determined via its algorithm that there was a high probability that Reema had cheated. The AI had used micro expressions around the eyes, measurements of pupil dilations, and pupil orientations derive its assessment. The algorithm did not take into account cultural differences, or fully account for skin tone. Reema's room also contained some posters and religious imagery on her walls to remind her of her home in Kabul.

EyeThentic's automated data sharing platform also provided information to U.S. Law Enforcement and Intelligence Agency models which used EyeThentic's data to feed into their threat models. The data was anonymized but was included in their facial recognition and pupil analysis models at border entry points and in biometrics databases.

Reema passed the test easily. But based on the flags raised by EyeThentic she was given a failing mark and her professor referred her to the honor council. She won her honor council hearing but was forced to switch to another professor's course at a less convenient time. Two years later when she was returning from a university service-based study abroad to Europe to focus on global public health she was flagged at U.S. Customs and border control and taken in for additional questioning. Again, she was released, but the experience was traumatic. She didn't know why she has been stopped and put into a room for additional questions after having just

worked in health clinics to help people, but what she didn't know what that her anonymized biometric data combined with her facial profile from EyeThentic had identified her as a potential risk. Reema graduated from the university and did eventually go to and graduate from medical school. But she never quite forgot how she was once asked to sacrifice her dignity to take a test, and she never did learn why she was profiled while returning from a study abroad program trip.

The case above is not science fiction. During the Covid-19 pandemic numerous universities and secondary schools around the world began implementing anti-cheating software that used gaze tracking. Eye gaze-tracking uses automated systems to measure and analyze the movements of a subject's eye and face determine emotions, attention, and even intent. The use of gaze tracking has proven a fruitful field of research that has branched out and facilitated advances in medical health, psychology, sports performance, computer user interaction experiences, marketing, and as examined above in proctoring of examinations to name just a few of the many use cases.[1] Gaze tracking technologies have been pervasive in science fiction for several decades with one of the most prominent examples of the technology being implemented in the 2002 Sci-Fi thriller *Minority Report*. In that movie gaze-tracking was leveraged for a variety of tasks from attention analysis for marketing to the tracking and identification of individuals using subsets of the technology such as retinal analysis. In the movie the technology is so advanced that John Anderton played by Tom Cruise must have his eyes removed and switched with a donor's eyes so that he can unravel the mysteries of the plot line. The present state of gaze-tracking technologies are not on the level with those forecasted in *Minority Report,* but they are increasingly being incorporated into everyday technologies from mobile devices to cars.

All users of modern mobile devices use some form of face scanning and gaze tracking technology to securely log users into their accounts. Apple's Face ID functions as a combination facial recognition system and gaze tracking system that places infrared markers on your face and uses the positioning of those markers to determine both whether the user seeking access authentication is the person whose face matches the information stored on the device and whether that individual is actively engaged with device, i.e. their eyes are open and looking at the screen.[2] Such technologies ensure the security of mobile devices and have become increasingly resilient to spoofing attacks such as masks.[3]

One area of research where gaze tracking has become particularly important is in the use of automobiles. As cars, trucks and other mobility devices increasingly incorporate automation devices including lane keep assist, breaking, self-driving etc. it becomes increasingly necessary to ensure that the operator of the vehicle retains their attention on the road and does not fully

[1] Lisa Graham et al., "The Eyes as a Window to the Brain and Mind," in *Eye Tracking, Background, Methods, and Applications*, ed. Samuel Stuart, Neuromethods (New York, NY: Springer Nature, 2022), 1–14, doi:10.1007/978-1-0716-2391-6.
[2] https://support.apple.com/en-us/HT208108
[3] Hao Fang et al., "Surveillance Face Anti-Spoofing," *ArXiv*, January 3, 2023, doi:10.48550/arxiv.2301.00975.

allow the automated systems to operate without human oversight. Gaze tracking technologies are increasingly incorporated into cars that use advanced self-driving or automation technologies to provide reminders and cues to the driver of a vehicle to keep their attention focused on the road.[4] When these technologies identify a vehicle operator as inattentive, they can even go so far as to disable the automated driving features. As automated vehicles are increasingly used on roadways the use of eye tracking of drivers can be used not only as a gentle reminder to remain attentive but might also be a liability shield to protect car and software manufacturers in the event of an accident.[5]

Gaze tracking has also played a significant role in military systems including attack helicopters and fighter jets. The use of gaze tracking has done several things. First, it has allowed the pilot to offload manual tasks often requiring the use of hands to the eyes. Second it has allowed the pilot to focus on targets for engagement without losing operational awareness. The use of eye tracking has been particularly well-studied within military operations and use cases including the use of Apache attack helicopters.[6]

Moving beyond device security and attention monitoring in vehicles gaze tracking technologies are increasingly being leveraged within the health care industry and medical research fields to provide insights into disorders and diseases that might otherwise go unnoticed. Bibliographic analysis of research in the field of gaze tracking indicates that the technology is being increasingly used to detect autism spectrum disorders, schizophrenia, depression, anxiety, Parkinson's disease and Alzheimer's disease.[7] Iterative gaze tracking has also been deemed a method for identifying complications associated with Type 1 diabetes including diabetic neuropathy (damage to ocular nerves).[8]

Each of the above use cases demonstrates both the utility and scope of a growing field of technology. Yet there are substantial dark sides to the research including violations of privacy, disclosure of information without knowledge or consent, the discovery of health issues without a subject's knowledge and more. There are pervasive examples of gaze tracking technology being increasingly implemented to assess worker productivity,[9] assess honesty in individuals being

[4] Christer Ahlström et al., "Eye Tracking in Driver Attention Research—How Gaze Data Interpretations Influence What We Learn," *Frontiers in Neuroergonomics* 2 (2021): 778043, doi:10.3389/fnrgo.2021.778043.
[5] David Vetturi et al., "Use of Eye Tracking Device to Evaluate the Driver's Behaviour and the Infrastructures Quality in Relation to Road Safety," *Transportation Research Procedia* 45 (2020): 587–95, doi:10.1016/j.trpro.2020.03.053.
[6] David B. Durbin and Jamison S. Hicks, "AH-64D Apache Longbow Aircrew Workload Assessment for Unmanned Aerial System (UAS) Employment," 2009, doi:10.21236/ada494123.
[7] Gianpaolo Zammarchi, "Application of Eye Tracking Technology in Medicine:A Bibliometric Analysis," *Vision* 5, no. 4 (2021): 56, doi:10.3390/vision5040056.
[8] Francesca D'Addio et al., "Abnormalities of the Oculomotor Function in Type 1 Diabetes and Diabetic Neuropathy," *Acta Diabetologica* 59, no. 9 (2022): 1157–67, doi:10.1007/s00592-022-01911-1.
[9] https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/

interviewed,[10] and tracking attention of students taking exams in online settings.[11] Reema's story above is a story experienced by thousands of students since 2019. It is a story of trying to do the right thing but being forced to use a technology that pushes the limits of privacy and personal spaces. In extreme cases it can give strangers a view into our personal spaces that were once the shelters or places of refuge from the wider world. These technologies can fail to take into account the human cost and toll on the individual being analyzed. Being unable to look away from a computer screen while taking a test can include limitations of normally bodily function and movement including preventing test takers from using the restroom or in extreme cases constrain those suffering from testing anxiety to a desk and lead to adverse health effects.

The technologies are frequently marketed as unbiased assessments of human performance. They are viewed as digital intermediaries into the world of tests, job interviews, driving, and health care. Yet this view of an unbiased machine gaze is not entirely accurate. Many of the systems collect, store, and share large volumes of data on the individuals being examined. Sometimes these data are anonymized, and sometimes as in the case of tests the data are not anonymized and are subject to post action review by strangers or faculty. Where data is generated and shared it is often done so without the subject's full knowledge or comprehension of its application and use in extended cases. Recognizing these challenges and the multitudes of use cases raises important questions.

Question #1

As computers increasingly incorporate new sensors to detect objects and make sense of the world around them the line between digital spaces and non-digital spaces becomes increasingly blurred. Gaze tracking can occur in several ways ranging from the use of cameras, lasers, or infrared sensors. Each of these sensors collects substantial volumes of data which are then fed into algorithms which make 'decisions'. These algorithms operate in a class of machine learning and artificial intelligence that allows the computer to use the sensed data to make inferences about the subject being sensed. These inferences are predicated on data derived from training datasets. Training data is often collected from known repositories of subjects previously categorized. Frequently these training datasets reflect the social, cultural, religious, and ethnic characteristics of majority populations within a state. What are some of the challenges of using training data in the gaze tracking applications listed above? How might they disadvantage certain religious, cultural, or ethnic groups? What are the implications of applying training data trained specific population characteristics on another population?

Question #2

In the case example at the beginning Reema is faced with a moral dilemma. She must decide whether to adhere to her religious tradition by continuing to wear her hijab and represent her

[10] https://www.washingtonpost.com/technology/2021/11/15/lie-detector-eye-movements-converus/
[11] https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/

faith or to remove her hijab to take a test to meet the needs of an algorithm. She discusses her initial quandary with her parents and her professor. She eventually decides to remove her hijab reasoning that it is only a computer algorithm viewing her and not another person. Yet we find out that this is not entirely the case. We also learn that the data collected on Reema is shared within other databases. What should or could Reema have done under these circumstances? Was she justified in her concerns? What are the implications of adjusting one's moral framework for digital system as opposed to a human operator? Have you experienced similar challenges with anti-cheating software?

Question #3

Reema's professor is unyielding in his approach to mandating the use of anti-cheating software. He adheres to an ethical framework that privileges honesty in test taking environments over the moral concerns of his student. His justification is rooted in a desire to produce students who have a strong working knowledge of the material he is teaching. He sees this as a critical first step in creating well-trained medical professionals. Is Reema's professor wrong? How might he have handled the situation better to more appropriately accommodate Reema's concerns? Is it ethical to use anti-cheating software if the data is only analyzed by machines and the data is kept private? What if the data is analyzed by human operators and machines but the data remains private? What if the data is analyzed only by machines but the data is anonymized and sold to third parties? What if the data is analyzed by machines and human operators and the data anonymized data is sold to third parties? What are the ethical considerations from the perspective of the faculty member and how do they conflict with the moral, ethical, and privacy concerns of the students?

Question #4

Gaze tracking and similar technologies expose our physical bodies to a form of digital intrusion and data collection that has previously not been encountered. Whereas when meeting a person that might look into your eyes they are doing so only with their individual prior experiences and knowledge to inform them. They are unable to retain that data beyond the limits of human memory capabilities and are unlikely to detect most health issues that might be hiding within your eyes or gaze. Yet computers equipped with gaze tracking are able to collect retain and analyze data on human eyes and gaze that can be compared to data collected from other individuals residing in datasets. This enables computers to use algorithms to make inferences about trained behaviors or conditions that might otherwise go unnoticed. Is collecting gaze related data about an individual with their consent a violation of privacy? What if that collection is under a form of duress such as taking a test, at an arrest, or to operate a motor vehicle? Is gaze tracking a privacy violation? If so, how? If not, why not?

Question #5

The case above and the examples below the case list many of the ways in which gaze tracking is advancing and becoming part of our daily lives through its incorporation into a diverse array of

technologies. Having learned more about gaze tracking and its capabilities what are your thoughts on the technologies and associated applications? Do the benefits of such technologies outweigh the costs? Are there redlines that should not be crossed with the technology?

Reflecting on the Gaze of Others

> *"The eye is the window of the soul, the mouth the door. The intellect, the will, are seen in the eye; the emotions, sensibilities, and affections, in the mouth. The animals look for man's intentions right into his eyes. Even a rat, when you hunt him and bring him to bay, looks you in the eye."*
>
> ~ Hiram Powers 19th Century Neoclassical Sculptor

Many a poem, quote, and religious text has focused on the eyes as a "window to the soul." For most of human history this window has been viewable only by our fellow man or woman. Gazing into the eyes of another has formed the literary basis for many a story, and tales of love, honesty, deception and more have arisen from such glances. The formal study of eyes and their gaze dates back hundreds of years to the 17th century and the famous German astronomer Johannes Kepler. With the invention of photography, the collection and analysis of data on the eye gained new steam in the late 19th and early 20th centuries. Yet it is the invention of the computer, the development of advanced sensors, and algorithms, that have transformed one human gazing into the eyes of another into a systematic, mathematical approach to see into the souls of others. During this search scientists and engineers have unlocked implications for health and mobility, marketing and even honesty. The instruments of analysis are no longer large sensors in labs, but rather small cameras or sensors on mobile phones or laptop screens. The window to the soul is now open to the mechanical devices of man to analyze, probe, record, share, and exploit. Increasingly advanced gaze tracking technologies are just over the horizon. In 2024 Apple plans to introduce its Vision Pro mixed reality headset which incorporates dramatic advances in gaze tracking to enable spatial computing. Other firms including Tobii have developed gaze tracking glasses for use in research and software development. Each new technological advance with gaze tracking brings with it challenges of accountability, inequality, transparency, and privacy.

Accountability: Gaze tracking systems pose multiple concurrent accountability issues. These issues vary by use case. At their most basic, accountability issues and gaze tracking are associated with the analysis of collected data in comparison to large training models. Gaze tracking systems are collecting data on a single individual and comparing that data against data in training datasets. As the use case varies the implications of correlations between different datasets can be significant. Gaze tracking in health care instances leveraging models can lead to identifications of disease or psychological conditions requiring treatment. These identifications can substantially impact individuals' quality of life, result in diminished access to employment, or opportunities for care. In cases where gaze tracking is used to ensure driver situational awareness it can serve as a

partial liability shield that might undermine claims against a self-driving car manufacturer of software developer. If the gaze tracking software makes a claim that a driver was inattentive, and the self-driving software was faulty the blame for a potential accident might be entirely shifted to the driver and away from the developers or manufacturers. In weapon systems a faulty gaze tracking system might lead to the targeting of unintended targets which might result in war crimes or casualties. In test taking scenarios it might lead to the identification of cheating in individuals with anxiety, health issues, or other extenuating factors that might undermine the accuracy of the gaze tracking system. Being able to audit the algorithm and its subsequent interpretation are critical to ensuring and improving accountability over time. These technologies are still largely in their infancy and are subject to failures both of the sensors and of the algorithms. Ensuring accountability remains a crucial aspect of using gaze tracking.

Inequality: Everything from the algorithms and datasets used to train and analyze data collected to the design and the development of the sensors associated with gaze tracking pose issues that can impact inequality. Where datasets are trained on majority populations their characteristics are likely to heavily influence learning models used in interpreting the data derived from gaze tracking sensors. Systems trained only on white, western faces are more likely to misinterpret the facial expressions of individuals with different skin tones and from different cultural or social backgrounds. The inference models used are only as good as the data that informs them. Because most datasets are limited in scope, they will likely overlook certain characteristics. The issues of inequality are not isolated to the data used to train models. The sensors and devices used in gaze tracking can themselves be prone to reinforcing bias or other forms of inequality. Systems which use cameras, infrared, or even lasers can misinterpret or underrepresent reactions based on the reflectivity or absorption of light based on melatonin levels in an individual's skin. There has been little research to date on the way in which differences in biological characteristics impact the fidelity of gaze tracking sensors. This is likely to lead to results from gaze tracking that less accurate where the impact of novel conditions undermines the accuracy of certain sensor types. Finally, there is an inequality of access. As issues with data diversity and sensor fidelity improve there will remain issues of access across social, ethnic, and economic groups. This could be particularly harmful in the medical field where individuals in minority groups are less likely to receive access to newer technologies that might help them identify issues of concern. Because fewer members of such groups are exposed to these technologies their data does not feed back into training datasets or into a more robust understanding of the fidelity of the sensors. The result is a pernicious loop of inequality.

Transparency: Gaze tracking generates a new data source. A source that is often private and intimate to individuals. While the poets, artists, musicians, and authors spoke of a window to the soul, the reality is that a person's gaze does reveal traits that they may wish not to reveal publicly. Such information might be health related or even as simple as tells in a game of poker. Information derived from gaze tracking can be extremely personal. Ensuring that individuals know what data is being collected; how it is being stored; who has access to that data and a bevy

of associated questions are key to understanding how transparent gaze tracking applications and their underlying infrastructures are. Increasingly important will be accurate information on the accuracy of gaze tracking to identify health related concerns, cheating, attentiveness and more. Transparency on the information and findings being represented is critical to ensuring that gaze tracking progresses within an ethical framework as technologies improve.

Privacy: This case analysis closes by looking at privacy and returning to Reema's case. Many use cases of gaze tracking are inherent violations of privacy. Requiring users taking a test to show their private space, to remove head coverings, to force them to keep their gaze on a computer screen for an extended period are all clear privacy violations. Whether gaze tracking in private spaces is fully automated or provides information to human users it constitutes a violation that should be weighed against all other reasonable options and outcomes. In Reema's case as has been the case of so many other students there is a power disparity between the professor and the student that allows the professor to impose a technology on students that can violate privacy and upset moral or other ethical frameworks. The technology is not benign. It opens a window into one's home and into their soul in a way that can feel like and be a significant violation. When the data associated with gaze tracking is not kept private or when unexpected persons even with legitimate purposes have access to that data it can be intrusive. Whether it is gaze tracking for a test, driving attentiveness, or other use cases understanding the privacy implications of the technology are important.

Ahlström, Christer, Katja Kircher, Marcus Nyström, and Benjamin Wolfe. "Eye Tracking in Driver Attention Research—How Gaze Data Interpretations Influence What We Learn." *Frontiers in Neuroergonomics* 2 (2021): 778043. doi:10.3389/fnrgo.2021.778043.

D'Addio, Francesca, Ida Pastore, Cristian Loretelli, Alessandro Valderrama-Vasquez, Vera Usuelli, Emma Assi, Chiara Mameli, et al. "Abnormalities of the Oculomotor Function in Type 1 Diabetes and Diabetic Neuropathy." *Acta Diabetologica* 59, no. 9 (2022): 1157–67. doi:10.1007/s00592-022-01911-1.

Durbin, David B., and Jamison S. Hicks. "AH-64D Apache Longbow Aircrew Workload Assessment for Unmanned Aerial System (UAS) Employment," 2009. doi:10.21236/ada494123.

Fang, Hao, Ajian Liu, Jun Wan, Sergio Escalera, Chenxu Zhao, Xu Zhang, Stan Z Li, and Zhen Lei. "Surveillance Face Anti-Spoofing." *ArXiv*, January 3, 2023. doi:10.48550/arxiv.2301.00975.

Graham, Lisa, Julia Das, Jason Moore, Alan Godfrey, and Samuel Stuart. "The Eyes as a Window to the Brain and Mind." In *Eye Tracking, Background, Methods, and Applications*, edited by Samuel Stuart, 1–14. Neuromethods. New York, NY: Springer Nature, 2022. doi:10.1007/978-1-0716-2391-6.

Vetturi, David, Michela Tiboni, Giulio Maternini, and Michela Bonera. "Use of Eye Tracking Device to Evaluate the Driver's Behaviour and the Infrastructures Quality in Relation to Road Safety." *Transportation Research Procedia* 45 (2020): 587–95. doi:10.1016/j.trpro.2020.03.053.

Zammarchi, Gianpaolo. "Application of Eye Tracking Technology in Medicine:A Bibliometric Analysis." *Vision* 5, no. 4 (2021): 56. doi:10.3390/vision5040056.