Student Occasional Paper Series No. 6 | January 2024

A Critical Examination of Gaze Tracking Technologies

By Sebastian Bukvic

Editor. Aaron Brantly

Abstract

The main objective of this research paper is to analyze the recent and future developments in eye gaze-tracking technologies and critically evaluate its usage. Eye tracking systems and software are not new. However, applications of the technologies have not seen widespread use until recently. These recent use cases are leading to a variety of considerations regarding the ethics, legality, security, and privacy of these systems. Most personal devices such as smartphones, laptops, tablets, and even some gaming consoles have some form of camera. Data derived using these devices from a person's eyes and facial features can reveal a substantial amount of information. This paper questions whether or not this technology is promising or whether it poses underlying risks that outweigh its potential benefits. This research paper analyzes past, present, and future eye gaze-tracking use cases and examines applications of the technology in relation to the topics of ethics, legality, security, and privacy, and lastly proposes policy options for consideration.

Introduction

In a world where data, communication, and associated technology systems are rapidly improving and changing, it is critical to understand how technologies may affect individuals, and societies. Eye gaze-tracking and facial recognition technologies are an emerging field of technologies that are becoming increasingly common. Many phones, tablets, laptops, and even handheld gaming consoles all have some level of capability for eye gaze tracking. Beside personal devices, eye tracking occurs in many different

contexts, from China where facial recognition data collection assists in the identification of its citizens, to use of WorldCoin cryptocurrency, where a retinal scan is required to verify a person's identity as a cryptocurrency owner (Gent 2023). Considering that eye tracking is prevalent in many settings, it is increasingly pressing to understand the extent of the benefits and problems associated with this suite of technologies.

This research synthesizes current knowledge on the usage of eye gaze-tracking and facial recognition technology and its impact on ethical, legal, security, and privacy issues. This research identifies the strengths and weaknesses associated with eye tracking technologies and whether these technologies are safe for widespread adoption in consumer technologies. The following research also provides background knowledge on the history of eye tracking, its functions, applications, and possible future developments. The analysis below concludes detailed discussion of the costs and benefits of eye gaze-tracking technologies.

What is Eye Gaze-Tracking?

According to Morimoto and Mimica, eye gaze tracking devices are systems that estimate the direction of a person's eye-sight or gaze (2005). Furthermore, Chennamma and Yuan define eye gaze tracking as, "the measurement of eye movement/activity and gaze (point of regard) tracking is the analysis of eye tracking data with respect to the head/visual scene" (2013). Due to the importance of an individual's eyes in relation to facial movements, eye gaze tracking is a critical part of facial recognition technologies. Eye-tracking techniques have existed for centuries, with major strides in that field beginning in 1947, in the aftermath of World War Two (Ould Mohamed, Perreira da Silva, and Courboulay 2007). Since then, applications and advancements in eye gaze-tracking, and facial recognition, have exponentially increased, as seen with software and products like SeeSo, WorldCoin, and the Apple Vision Pro, all of which have utilized eye tracking in different ways. These examples of eye gaze-tracking technologies will be further expanded upon in the following sections. Eye tracking data can be used in various fields including health, gaming, military, spatial computing and more.

Historical Developments and Practices of Eye Tracking

While mankind has studied eyes and eyesight for thousands of years, the topic of vision and how vision biologically functions in humans was thoroughly documented at the beginning of the 17th century (Simon 1975). During this period, Johannes Kepler published Astronomiae Pars Optica, a scientific publication where he theorized about human vision and the role of different eye features (Simon 1975). Kepler believed that light rays are not emitted by the eye, as was the common belief by many scientific minds, rather, Kepler theorized that light rays reflect off objects and then enter the eye, which ultimately results in the visual appearance of objects (Simon 1975). Many centuries later, some of the most impactful strides in the field of gaze tracking occurred in 1947, when a group of scientists published research on the eye gaze-tracking of over 500,000 frames of 40 pilots in various flight settings (Mohamed, Da Silva, and Courboulay 2007). These authors concluded that "It is reasonable to assume that frequency of eye fixations is an

indication of the relative importance of that instrument. The length of fixations, on the contrary, may more properly be considered as an indication of the relative difficulty of checking and interpreting particular instruments. [...] If we know where a pilot is looking, we do not necessarily know what he is thinking, but we know something of what he is thinking about" (Mohamed, Da Silva, and Courboulay 2007). The results of this work led researchers and scientists to develop studies with better instruments and data collection techniques. Throughout the latter half of the 20th century, eye tracking devices improved in accuracy and complexity, with head-mounted trackers becoming a popular tool for data collection. Until recently, eye tracking studies were often conducted at military labs due to the complexity and cost of tracking devices (Mohamed, Da Silva, and Courboulay 2007). This resulted in eye tracking data being primarily used to help with targeting devices for military applications (Mohamed, Da Silva, and Courboulay 2007). Today, eye gaze-tracking is often paired with facial recognition systems, the latter of which has seen a plethora of applications, especially facial scans for security, with eye gaze-tracking technology use cases themselves growing as well, albeit at a slower pace.

How Eye Gaze-Functions

Gaze-tracking data collection can be gathered continuously. Yet, how data are collected varies by technique or device used. Collecting eye movement data can be sorted into two main methods, invasive and non-invasive tracking methods (Chennamma and Yuan 2013). Head-mounted and physically attached eye tracking devices are considered invasive tracking methods. Non-invasive tracking methods and devices carry the following criteria: they allow natural head movement, they work with a variety of eye shapes, glasses, contacts, or other possible data collection obstructions, they should be portable, and they should provide real-time data (Mohamed, Da Silva, and Courboulay 2007). A person's laptop or computer webcam would be considered a non-intrusive eye tracking device, albeit a straightforward one that has varying probabilities of inaccuracy depending on the device used on a case-by-case basis. Both the intrusive and non-intrusive methods of eye tracking are further sorted into two categories based on the form of light they use, ambient light or infrared light (Ould Mohamed, Perreira da Silva, and Courboulay 2007). Eye tracking methods include electro-oculography, scleral search coils, infrared oculography, and video oculography (Chennamma and Yuan 2013). Electro-oculography tracks an individual's eyes by measuring electric field movement when the individual's gaze shifts. It uses sensors in the form of electrodes placed around the eyelid. This method is invasive with the numerous sensors placed around the eye, and as such accuracy varies with the positioning of the sensors, however, the benefits of this method of eye tracking are that it is inexpensive and will detect eye movements even when the eyelid is closed (Chennamma and Yuan 2013).

Similar to electro-oculography, scleral search coils require an invasive placement of the eye tracking device, in this situation, the sensor is similar in appearance and feel to contact glasses, however, the scleral search coil contacts contain small wire coils that measure the magnetic fields associated with eye movement (Chennamma and Yuan 2013). While this method is extremely accurate and efficient, it is considerably invasive, with an object being placed in one's eye that may require use of local anesthetic

(Chennamma and Yuan 2013). Infrared oculography uses sensors placed on spherical glasses to bounce infrared light off an individual's sclera and measure the difference in reflected light (Chennamma and Yuan 2013). The benefits of this are that eye tracking can be performed in low to no light settings. However, the primary drawback of this method is that eye movement can be measured only between a positive and negative 35 degrees horizontally and a positive and negative 20 degrees vertically (Chennamma and Yuan 2013). Under the video oculography method umbrella, the most common and modern form of eye tracking devices are video-based eye trackers, that use infrared light to illuminate the eye that causes a glint on the cornea of the eye, known as a corneal reflection (Chennamma and Yuan 2013). This corneal reflection is then used as an estimated reference point for gaze detection. Video-based eye trackers vary in number of cameras, with single camera systems being the most common, but also the most inaccurate. The more cameras used to collect eye data, the more accurate the system is. More cameras are also important because they allow the individual, whose eyes are being tracked, to have increased freedom of movement during data collection.

The Applications of Current-Day Eye Tracking

Analyzing present implementations of gaze-tracking informs the future development of this technology. The world of eye tracking is rapidly developing and expectations of future innovations in this sector are expected. Contemporary eye tracking applications vary from programs in GitHub software repositories to commercial applications such as anti-cheating proctoring apps, and even systems to unlock a personal device through facial recognition. Furthermore, Venugopal, Amudha, and Jyotsna, list the present applications of eye tracking technology as follows: website usability, marketing research, assistive technology for disabled peoples especially regarding Amyotrophic Lateral Sclerosis (ALS) patients, digital job training scenarios, analyses for human behavior, developmental psychology, neuroscience, and human-environment interaction research (Venugopal, Amudha, and Jyotsna 2016). The medical sector can use this data to find underlying diseases and improve diagnostic interpretation (Brunyé, Drew, Weaver et al., 2019), and the security sector can use this data to authenticate and prove someone's identity (Kavusi, Maghooli, and Haghipour, 2023). For example, Morimoto and Mimica state that the analysis of eye gaze-tracking data can provide insight into "ophthalmology, neurology, psychology, and related areas to study oculomotor characteristics and abnormalities, and their relation to cognition and mental states" (Morimoto and Mimica 2005). In addition, Punde, Jadhav, and Manza, list the following companies as producing professional and commercial head-mounted or mobile eye tracking products: Tobii, SMIVision, EyeLink, Interactive Minds, Imotions, Mirametrics, and EyeTech (2017).

The usage of these systems and technologies defines what the future may hold, however, it will also define what potential consequences may arise due to the mass adoption of eye tracking and facial recognition systems. For example, an individual's age, gender, race, sexual preference, body mass index (BMI), hormonal cycle, overall health, and focus on a task, can be extrapolated through the analysis of scanpaths, pupil dilation, and microtremors from collected eye data (Liebling and Preibusch 2014). It is rare to find a

workplace or teaching environment without a requirement of some form of electronic device, from a smartphone to a laptop or personal computer. With an increased reliance on technology, it is important to prevent malpractice in the utilization of different hardware and software. Similarly, a key circumstance of intrusive technologies would be eye gaze-tracking and facial recognition systems, as they collect data on some of the most physically personal information about oneself, one's eyes and face. This data can be used further to reveal underlying attributes about oneself and most importantly, hidden behaviors as well (Liebling and Preibusch 2014). The following subsections will provide a brief overview of the existing applications of eye tracking technologies, their functions, and any notable concerns that arise with the usage of these technologies.

SeeSo Software by VisualCamp Co.

The SeeSo software by the VisualCamp company is an example of a transformative eye tracking technology, as it can be installed on most devices with a camera and screen, albeit, primarily mobile devices, that will allow users to interact with screen commands, movements, and selections, purely through tracking eyesight on the screen from the device camera. Beyond basic movement and selection interaction with a device, the SeeSo software advertises a variety of other functions that would allow users to better interface with their device as it is used in daily life such as gaze data-based recommendations.

The SeeSo software and related company appear to provide very professional and commercial grade products, as their industry clientele, investors, and partners include Kyo Won, LG U+, Chungdahm Learning, Visang, and Woogjin in the education sector, DoBrain - Learning Lab for Kids, Dotsoft, Salpha DTx, and dot in the digital therapeutics sector, and Millie's Library in the E-Reader sector (VisualCamp n.d.). The development team that manages SeeSo software is physically located in the United States, however, its direct parent company, VisualCamp Co, that oversees all licenses and copyrights, originates from Seongnam, South Korea (Clutch n.d.). VisualCamp specializes in Virtual Reality Head Mounted Displays (VR HMD), or virtual reality (VR) headsets, including their applications, advancements, and software (Clutch n.d.). Their applied research has been used in areas such as in the marketing research field, VR market, health and human performance, kinesiology, and educational industry (Clutch n.d.). In addition, they were selected by Red Herring as one of the most innovative 100 technology startups in Asia in 2023(Cho Jin-Young 2016).

VisualCamp has multiple industry investors and partners and is most notably known for its SeeSo software. The SeeSo software maintains itself as a software development kit (SDK) which can be easily integrated with a mobile device (VisualCamp n.d.). It provides eye control for the device and most importantly for understanding eye data privacy and security concerns overall, it collects this data (VisualCamp n.d.). According to the SeeSo website, "With SeeSo's eye tracking software and gaze analytics, you can know when users are looking, where they are looking, and for how long all in real-time," this statement illustrates the company objectives of the SeeSo software and potential concerns,

especially regarding the data collection aspect of these functionalities (VisualCamp n.d.). While the SeeSo software is best suited for smartphones and other similar mobile devices with iOS or Android, it can also be used with other platforms, including Unity, Web(js), and Windows C++, as well as other systems including tablets, laptops, and computers with the stipulation that all the aforementioned devices have webcam capabilities(VisualCamp n.d.).In the promotional video, SeeSo advertises that it can assist mobile device usage through five major features, eye scrolling, eye play and stop, gaze data based recommendations, eye navigator, and gaze analysis (VisualCamp 2020). The promotional video kept displaying slogans such as, "Welcome to Eye Tracking World" and "Develop your Eye Tracking World," indicating what goals and developments the company seeks to achieve in the future, if their software truly takes off and even inspires other companies to the same (VisualCamp 2020).

The following functions in the software could assist mobile device usage, eye scrolling simply put is scrolling up and down a mobile app or website using eyesight, likewise, eye play and stop is fairly straightforward, which means when one's eyes look away from the screen, whatever video is being played, pauses (VisualCamp 2020). The gaze data-based recommendations offer a more complex and possibly worrisome feature; the gaze data based recommendations feature tracks an individual's eyes on the screen as they browse websites and online stores to track what items users paid the most attention to and what topics or items interested them the most (VisualCamp 2020). As such, SeeSo can help users find similar items they liked or have the same items they showed interest in reappear in their suggested searches similar to that of website cookies (VisualCamp 2020). The eye navigator feature helps the user navigate their screen like a mouse or trackpad (VisualCamp 2020). Gaze analysis is similar in functionality to the gaze data-based recommendations but is essentially a more in-depth data collection feature (VisualCamp 2020). Expanding upon the gaze analysis explanation, akin to the gaze data-based recommendations, the gaze analysis feature tracks what interests a user but to a further extent as it does not limit gaze data collection to only shopping related tasks, rather, the promotional video displays that it builds an online interest persona of sorts based on what subjects a user focuses on the most while using their mobile device (VisualCamp 2020). The visuals in the SeeSo promotional video displayed what appeared to look like a heat map on a phone that depicts how long a user was looking at something on their screen and what level of interest they had in that item (VisualCamp 2020).

Regarding privacy and security concerns, some SeeSo features stand out from the rest due to their proclivity to disregard privacy of personal information. First, the SeeSo developers openly state on numerous occasions that one of the primary primitive functions of the software is to collect data. Information on how the data is collected, where is the data being stored, and for what purposes is the data being used for is hidden behind a paywall and licensing agreement that would allow a customer to gain access to the software. Furthermore, if the SeeSo software utilizes machine learning techniques in the case of the gaze data-based recommendations and the gaze analysis functions alongside data collection, the VisualCamp company will get personalized and ever-growing online profiles of individuals. These two functions of SeeSo could be seen as the

most concerning features of the software as they collect very personal information about individuals and then customize their content without their direct influence or permission. The widespread implementation of this program could possibly provide one of the worst violations of privacy in personal technology in recent years as it would collect data about everything regarding one's eye gaze and all the personal information one's gaze, and face could display.

If this software is implemented in most devices, aside from physically covering the camera, not much else could be done to prevent eye data collection. It is further important to know who is collecting personal data. The SeeSo developers and the VisualCamp Company who would be the primary proprietors of this data are mostly located in the United States of America and South Korea, however, after checking the VisualCamp Co website, or more specifically, the VisualCamp Team section of the website, one of the four main executives of the company works as a part of the Chinese branch of the company as the Chief Marketing Officer and Division Leader (VisualCamp n.d.). The Chinese branch of VisualCamp Co is a branch that is not listed very openly on their website. Considering that China has had a track record of manipulating and targeting different countries, people, and their own citizens through personal data collection and tracking, this brings with it a concern that Chinese authorities could possibly gain access to people's eye data, online personalities, private communications, behavioral analyses, and other potential personal descriptors (M. S. Chen 2019; J. Chen and Xu 2017).

While the words 'consideration' and 'concern' have been used extensively throughout this section, it is not to say that the SeeSo software will bring about the end of privacy and security. Rather it implies that the usage of those words and worst-case scenario circumstances are there to illustrate the potential consequences that this and similar software or programs could have if they succumb to deleterious behaviors, such as the selling of data. Considering SeeSo is currently not widely used, the risks posed by SeeSo are minimal.

WorldCoin

In the late Fall of 2022, Moiz Ahmed displayed the first showing of his brand-new cryptocurrency system, WorldCoin, in the Indian city of Bangalore (Gent 2023). Here, he proposed a completely new way of earning cryptocurrency as well as validating a crypto holding account (Gent 2023). Ahmed introduced what would be called "the Orb," a soccer ball-sized metal sphere containing the technology to perform a detailed scan of one's iris and collect all associated data. The Orb's concept was designed to entice potential WorldCoin customers with 25 free coins and an offer of a secure and unreplicable crypto account (Gent 2023). The WorldCoin company's vision was to provide a welcoming opportunity for the masses into the world of cryptocurrency and create the most traded and widespread global currency, which would be further supported by the offer of what appears to be free money (Gent 2023). When data as personal and self-identifying as one's irises is now being collected by a major company, such unprecedented access to personal data requires checks and balances that will ensure the protection of civil rights

and privacy. Since that press conference, WorldCoin has seen both a rise in interest amongst the public and an increase in scrutiny due to privacy, transparency, and security concerns mostly as a result of WorldCoin's biometric data collection approach (Gent 2023). Sam Altman, a tech multimillionaire and CEO of OpenAI, the company behind ChatGPT, is one of the founders, co-owners, and largest investors of WorldCoin, having already invested well over 115 million dollars into the crypto project. Currently, with investments from multiple individuals and firms, WorldCoin stands at about a 1-billion-dollar evaluation. According to Gent, WorldCoin's original company vision has concerningly changed since its first press release, as its developers started increasingly sharing user data with third parties for a variety of identity-focused applications (Gent 2023).

Additionally, according to testimonies of the WorldCoin CEO Alex Blania, a secondary, albeit long-term, goal of WorldCoin since 2020 has been the redistribution of global wealth to the masses which could occur if WorldCoin gains a much higher level of adoption and value (closer to that of Bitcoin and Ethereum) (Gent 2023). The ethical issues of WorldCoin arise when discussing the topic of 'informed consent' in relation to verifying one's WorldCoin crypto holding account with the 'Orb.' If an individual does not understand that they are signing up for a global identity system and surrendering personal data, they have little to no means of backing out and retrieving that data. WorldCoin may appear to be an average cryptocurrency, however, the necessary provision of highly sensitive biometric data makes it unique in comparison to other crypto counterparts. Additionally, Gent describes how WorldCoin's highly advanced security and data protection measures have been exploited in the past, providing yet another concerning issue with this cryptocurrency. Furthermore, Gent describes a testimony from Glen Weyl, a Microsoft Research economist, which states that concerning associations may result from WorldCoin's reliance on the usage of the Orb and its idea of a global identity system, creating a sense of a dystopian future rather than one that is inclusive, fair, and promising (Gent 2023).

WorldCoin as a cryptocurrency project is not concerning in and of itself. However, the concept of the global identity system that it is wholeheartedly advertising may set a dangerous precedent for future identification systems. Current-day personal proofs of identity would commonly be passports or driver's licenses, which are associated solely with one's country of residence, whereas a global identity system would provide one's personal information, background, residence, possible history of crime, amongst other unique identifying information to any country or government in the world enrolled in this hypothetical system.

Ethics, Legality, and Privacy Issues of Eye Tracking

The issues surrounding the topic of eye gaze-tracking and facial recognition applications can be dissected into three categories, ethics, legality, and privacy, where privacy overlaps with security concerns. These three primary categories can assist in developing a broader view of the potential consequences eye tracking and related technologies may have in different environments and settings. These categories consist of the following

considerations in relation to eye tracking practices: how ethical are they, how legal are they, do they breach privacy, and to what extent is privacy breached by these practices. Liebling and Preibusch, described the idea that an individual's gaze and its associated data and behavior, is the most honest and difficult to fake biometric attribute "because it reveals the subconscious in ways that are difficult to control," (2014). In addition, they noted "we can disguise our voices to fool speech recognizers; alter our appearances with clothing and makeup, and change our keystrokes to defeat keyloggers; however, we have only partial control of our gaze," (Liebling and Preibusch 2014). Liebling and Preibusch further noted that "many of the sensitive attributes derivable from gaze data are not borne from what we look at, but how we look, which is harder to control," describing the innately invasive nature of the data these technologies collect. Eye tracking datasets also create information that can unique identify individuals; according to one study by Roman Bednarik, Tomi Kinnunen, Andrei Mihaila, and Pasi Fränti, a 60 percent accuracy of identifying individuals was achieved only by measuring the pupil diameters (in the grand scheme of eye data collection, measuring pupil diameters is very rudimentary in comparison to what these technologies can achieve) from one second periods while looking at a still object (2005).

As of 2012, eye identification models achieved accuracy percentages ranging from 58 to nearly 98 percent (Liebling and Preibusch 2014). The privacy losses of eye tracked data affect an individual's identity, in relation to biometric fingerprinting and the interests or personal reservations of said individual. Furthermore, the identity-assessment based on eye tracking can also obtain other personal attributes, such as age, health conditions, and other physiological and biological characteristics. Based on data collected by eye tracking, an individual's interests can be attained based on the movement and focus of the eye on different subjects. This can be used to develop a profile of a person's political beliefs, sexual preferences, culture, behaviors, morals, and values. Expanding upon this subject, Kröger, Lutz and Müller list the "possible inference(s) of personal information" into the following designated categories: gender, age, physical health, biometric identity, cultural background, mental health, personality traits, skills, mental workload, level of sleepiness, cognitive processes, and even drug consumption (Kröger, Lutz, and Müller 2020).

More specifically, the data captured by eye trackers can help diagnose concussions, Parkinson's disease, obesity, vision disorders, depression, PTSD, autism, eating disorders, extroversion, introversion, neuroticism, drug use, such as tobacco, alcohol, marijuana, MDMA, and cocaine, and even a preference for skills and abilities, such as sports, languages, math, and science (Kröger, Lutz, and Müller 2020). Liebling and Preibusch state that these breaches of privacy can be referenced with the term, violations of the "privacy principle of informational self-determination" (Liebling and Preibusch 2014). To further explain that term and a violation of that principle, these privacy concerns disregard an individual's ability to "determine for themselves when, how, and to what extent information about them is communicated to others," especially in circumstances where the consent of sharing information is unclear or miscommunicated (Liebling and Preibusch 2014). In a legal and law purview within the United States, this breaches actionable privacy protection; "actionable privacy protection is achieved through notice

and choice. Ubiquitous gaze tracking puts both principles at risk. First, users cannot voluntarily control their gaze; they are thus disempowered to choose to withhold their data. Second, there is no effective mechanism to communicate to users what information their gaze is leaking" (Liebling and Preibusch 2014).

A critical concern of this data is not centered only on its collection, but the proliferation of the information after the fact. The information from social media, messaging apps, and content creation websites is often sold to 3rd parties for advertising, marketing, and research purposes, often with a goal of creating more profits for the company directly in-charge of those applications. Using the analogy of retinal data being as unique to oneself as a fingerprint, having an individual's fingerprint information openly disseminated on the internet, among companies, and by marketing agencies, puts said individual's privacy and security at risk. This is especially true, where many biometric scanners, such as ones on modern phones or select laptops, function through the use of fingerprint recognition. If a phone or laptop were to be accessed by a third party, vast personal data that may have been stored on those devices could be leaked or stolen, ultimately resulting in financial loss, identity theft, malware, amongst other invasive and criminal consequences.

Furthermore, while facial scans are not the end-all, be-all for biometric security purposes, especially in comparison to fingerprint sensors, they have gained considerable traction. This is especially true regarding the newer Apple smartphone products, which currently lack any fingerprint scanning capabilities. Rather, these phones rely on a combination of an alpha-numerical password alongside the primary form of device access, a biometric facial scan. To help further explain the trend of biometric security systems relying more-so on iris-based scans, Marinović, Muzic, Čoklo, and Njirić (2011) stated, "The technology is so advanced that it has become economically viable and efficient, it is possible to perform the identifications by eye from 9 feet distance, you need 10 seconds to execute a scan, in a minute you can handle 30 people. In 2009 8% of personal biometric identification was based on the eye, in 2017 the fingerprint (currently the most common method) will decrease from the current 39% ratio to 27%, and identification through the eye will increase from 8% to 19%" (Marinović et al. 2011).

Ultimately, the outcome and widespread usage of eye tracking systems in the daily lives of billions around the world is not a guarantee, however, as Liebling and Preibusch stated, "with (the) decreasing cost of gaze trackers, pervasive eye tracking is likely to become reality." As such, it is important to understand the risks involved with these technologies and properly prepare for their usage, especially when the question of this technology's extensive proliferation is 'when will we see the consequences of this technology,' rather than 'if we will see the consequences of this technology' (Liebling and Preibusch 2014).

Prevailing Consequences of Eye Tracking and Facial Recognition Technologies

These previous sections of research analysis evaluated current day applications of eye tracking and facial recognition technologies and the potential ethical, legal, and privacy-oriented issues of these technologies. The following subsections will discuss the

consequences eye tracking and facial recognition technologies have on the state of global affairs. As mentioned earlier, eye tracking and facial recognition technologies are often used together for data collection, as facial recognition technologies require at least some form of rudimentary eye data capture system. Further, this section will examine whether this technology is 'setting a dangerous precedent for the future' and what are the possible negative outcomes. It will also assess the level of misuse of these technologies in the government sector, where facial recognition is being used to assist with the maintaining of surveillance states and ultimately the unethical monitoring of citizens' activities and identities. In summary, this section seeks to determine possible 'precedents' or consequences of eye tracking and give a glimpse into what the future may hold for this technology.

China - A Surveillance State

This research analysis provides information most imperative to those living in places that do not already have strict eye tracking capabilities enforced by the government, where it is not too late to promote ethical adoption of advanced eye tracking and facial recognition technologies. Furthermore, this review seeks not to metaphorically 'make a mountain out of a molehill,' but rather display the full capabilities of these eye-tracking systems, as well as the magnitude of their potential short-term and long-term consequences. To understand what consequences these technologies may pose, it is important to study the circumstances of privacy, legality, ethics, and security, or lack thereof, in current-day China through the usage of these technologies. As is the case today, arguably one of the best descriptions of China, in terms of privacy and security, would be, "surveillance state." In this context, surveillance means "watching over" or extensively monitoring personal information by collecting and analyzing data and inferring meaning (Lyon 2022). A surveillance state can then be defined as a country in which the government uses such information to restrict personal freedoms, privacy, and liberties, by enacting more social control and regulations. China's government has spent decades degrading personal freedoms, such as speech, privacy, expression, protest, and even religion. Over time, China has employed a variety of strategies that assist in their mass surveillance and monitoring goals, from internet restrictions and services that track communications, browsing history, and overall online presence, to entire networks of cameras that track individuals and their behaviors through advanced facial recognition technologies (Qiang 2019). China is currently the most developed surveillance state in the world. Even though North Korea is also well known for their pervasive surveillance and suppression of personal freedoms, it does not have the resources nor the technology to match the Chinese advancements in this field. The following questions must be asked: how is this facial surveillance technology being used in specific applications, how is the public reception of this intrusive technology, especially concerning the opinions of Chinese citizens themselves, and what implications arise as a result of these facial tracking systems?

According to Qiang (2019), China has been the world's fastest-growing user of surveillance cameras, systems, and programs through governmental actions (Qiang

2019). China's country-wide facial recognition system implementation began in 2010 and now has over 176 million surveillance cameras across China, with plans to increase that number to 626 million over the course of the next decade (Qiang 2019). To manage their entire network of millions of cameras, named the "Skynet" project, China has employed the use of AI to assist with the efficiency of identifying individuals and their physical features, such as height, clothing, and gender (Qiang 2019). Qiang explains that these facial recognition technologies currently in place in China alongside other surveillance systems such as voice recognition and DNA data, are also being used to marginalize and even target minority groups in China, especially the Muslim Uyghur population (Qiang 2019). In the Xinjiang province, where a majority of the ethnic Uyghur Muslim minority resides, surveillance technologies are employed to an extreme degree; all Xinjiang residents ages 12 to 65 have to participate in mandated DNA collection and testing, and provide their fingerprints, a voice recording, and a 3D image of themselves to get a passport (Qiang 2019). Furthermore, the social credit system currently being implemented in China relies heavily on the surveillance systems in-place.

Kostka, Steinacker, and Meckel, describe that while Chinese citizens are more accepting of these surveillance measures, most notably facial recognition tracking, approximately 83 percent Chinese citizens would like to be more in control of their data, and 75 percent would prefer more traditional methods of identification over facial recognition tracking (Kostka, Steinacker, and Meckel 2021). Proponents of facial recognition tracking often wager losing privacy for security and safety benefits. A similar trend is taking place in many countries across the world, including western countries such as the United Kingdom, Germany, and the United States. The primary challenge of this technology is that the benefits are more evident than possible harms these systems could have for the users. There is no consensus on what precedents and controls should be given to the government above the baseline of providing extra security, and whether or not the efficiency regarding security would in this case be substantial enough to warrant implementation. The implications of these tracking systems, especially if used for harmful purposes, could mean a constriction of freedoms and the right to self-determination. China is just one example of a state using facial recognition systems for the control and surveillance of its own citizens. However, if other countries follow a similar approach like China, their citizens, may suffer similar consequences.

What Could the Future Hold for Eye Tracking Systems?

Advancements in eye tracking technology are happening faster than ever before due to the changing needs of industry and technology users. The examples of such utilitarian functions are unlocking a device through a facial scan or virtual classroom environments proctoring exams by monitoring the student's gaze (through their device camera) to prevent cheating. As this technology improves, it will provide new ways for users to interact with the world around them. For example, new eye tracking technology may grant people a variety of ways to access and interface with the internet, the environment around them, such as is the case with augmented reality (AR) and virtual reality (VR). It can even provide security benefits such as in the case of locating criminals or wanted persons to prevent crime. For example, a 2020 study by Yang, Kim, and Jung, concluded that the

longer a potential robber's eye gaze focuses on different street environmental factors, such as balconies, windows, doors, and possible pedestrians, the lower the chance of a robbery actually occurring (Yang, Kim, and Jung 2020). As mentioned earlier, privacy is the most evident concern of developing and adopting eye tracking technology as irises and eyes are as unique to an individual as their fingerprints (Odu and Idachaba 2011). In fact, an iris scan is more unique to an individual than their DNA or genetic fingerprinting, which is described by Odu and Idachaba in their 2011 paper where they state that on average, 0.2 percent of the human population shares identical DNA whereas the iris is randomly formed during embryonic gestation (Odu and Idachaba 2011). However, unlike fingerprints or DNA, retinal data has the potential to be collected easier as the majority of the devices people interact with in their daily life have cameras and the ability to capture this biometric personal data. Currently, aside from a select few phones such as the Galaxy Note 7 and Alcatel Idol 3, a majority of phones do not possess a direct way to use iris data for security purposes, however, De Jesús et. al. in their 2016 study provided a methodology with 88.17 percent accuracy that would allow any modern smartphone with a front facing camera to use an iris scan as a form of password. As technology advances, so will the capabilities for assimilating facial and eye data, which can lead to several consequences, such as identity theft, personal physical and mental ailments, emotions, level of honesty, as well as an entire physical identity being revealed amongst a variety of other ramifications (Liebling and Preibusch 2014). The following sections will outline future developments of eye tracking technologies and focus on individual devices.

Apple Vision Pro

The Apple Vision Pro is often referred to as a "a spatial computer" as it is neither specifically an augmented reality (AR) or virtual reality (VR) device, but rather a combination of both with additional functionality. It was introduced to the public in June of 2023, setting a precedent for eye tracking and facial recognition technologies far into the future due to its revolutionary features (Apple 2023; Gans and Nagaraj 2023). The Apple Vision Pro device is described as a headset that augments the reality around an individual by serving as a mini computer and virtually casting different applications and windows into a surrounding environment in a way that would make those applications appear to be floating right in front of them (Apple 2023). However, because people cannot see through the headset, as one would, for example, with sunglasses or ski goggles, the Vision Pro scans a surrounding environment and projects into the interior lenses of the device making the Vision pro neither an AR or VR device. According to the promotional video, the Vision Pro has a variety of functionalities and promotes more efficient interfaces with different tasks including, but not limited to, photos and video (the 3D aspect of these features was extensively advertised), entertainment (such as watching movies, playing video games, and facetime), and work (advertised as making a desktop workspace interface simpler and more efficient) (Apple 2023). Since the Apple Vision Pro covers a majority of an individual's face during video conferences and facetime, Apple states that the device uses machine learning techniques to scan one's face and create a virtual model of themself that is seen when they are on a video call, similar to that of a

deep-fake video (Apple 2023). As an individual speaks and gestures, their virtual model will do the same (Apple 2023).

The key aspect of the Vision Pro that is of interest to this study is its unique and intuitive way of controlling the device; the Vision Pro is controlled through three primary actions, hand gestures, voice activation and command, and most importantly, eye gaze-tracking (Apple 2023). In this device eye tracking is primarily used to select applications and perform minor screen gestures and to detect whether a user looks away from the screen in order to display a closer view of their surroundings, for example, in the case of a person checking the notifications on their smart watch or interacting with a person in close proximity, the Vision Pro switches to a real time camera view (Apple 2023). In addition, an individual's eye tracking can be used to synchronize with other Apple devices such as a MacBook; when an individual looks at their MacBook laptop with the Vision Pro headset, it will quickly synchronize with the screen and files, which appears to be the case with most other newer Apple devices as well (Apple 2023).

The advertising campaign of the Apple Vision Pro by Apple itself may paint a picture of an advanced and futuristic technology for consumers. However, it is unclear what is the true reason for the creation of such a product when other less advanced devices fulfill most of the tasks the Vision Pro sets out to solve. In Gans and Nagaraj 2023 article, titled "What Is Apple's Vision Pro Really For," the authors provided many thoughtful insights to this subject, including, "VR meetings with avatars in pretty rooms do not provide information that is obviously more useful to those in the meetings that might arise from a Zoom call. AR glasses that provide text notifications as you walk around are increasing your cognitive load rather than decreasing it." (Gans and Nagaraj 2023) This example illustrates how this new technology could be centered on showing off its technological capabilities for public reception (Gans and Nagaraj 2023). Further referencing the authors in the aforementioned Harvard Business Review article, they stated, "The iPod was a digital Walkman. The iPhone was a connected iPod. The iPad was a bigger iPhone. The Apple Watch was a better smartwatch. And the Vision Pro is an unconstrained 3D screen. In the previous cases, the device is outgrown and becomes more than that initial use by enabling developer innovation. The Vision Pro is a welcome new experiment along a well-trodden path in computing" (Gans and Nagaraj 2023).

The Apple Vision Pro promotional video is about selling an expensive headset with extremely advanced and commercialized eye tracking and facial recognition technology, however, how could this set a precedent for future eye gaze-tracking applications, if at all? Major profit-driven companies peddling new technology and inventions can cause a chain reaction among other companies to follow suit. Perhaps eye tracking and facial recognition is the future for interfacing with personal electronic devices, certainly primitive forms of these technologies are gaining more traction as seen with newer smartphones using facial recognition as a form of digital password or lock-key.

Conclusion

This study provides a critical perspective on eye gaze tracking and facial recognition technologies and discusses their potential consequences. It is often difficult to predict what impacts may arise as a result of technological innovations. This is in part due to technological research and development being governed by entrepreneurial and political opportunities. For instance, while the Chinese government may be employing facial recognition tracking systems in order to provide more security and power for the government, implementing infrastructure for such ubiquitous data collection requires significant financial resources and political support. Similarly, private companies that are developing these technologies for profit. Currently, eye tracking technology is not fiscally difficult to produce, even with more advanced models, which would create an opportunity for their mass production and affordable manufacture, pending market demand. These technologies will be more pervasive in the next few years, as resources, research, and development have already been allocated to support these efforts in both private and government settings. However, the impacts, the consequences, and the lasting pervasiveness of these technologies beyond the near future are still unclear.

Based on the information included in this paper's analysis, it can be predicted that eye tracking technology will continue to grow and gain traction, becoming commonplace. Its integration into society will bring a combination of benefits and consequences. Additional research is needed to understand the value of this technology in individual applications, privacy risks, and strategies to manage them. This analysis also revealed that the literature about broader risks of this technology is scarce and mostly theoretical. Thus, primary research should be conducted to assess possible adverse outcomes of eye gazing technology's widespread implementation. Technological innovations have brought mankind prosperity and improved the quality of life, but not without adverse consequences. Certainly, eye tracking systems may not have the global impact of climate change. Yet, their potential societal impact may be just as profound. These anthropocentric impacts are likely to affect other facets of life and society. As such, eye gaze-tracking technology warrants continuous and thoughtful implementation.

Bibliography

Apple, dir. 2023. *Introducing Apple Vision Pro*. https://www.youtube.com/watch?v=TX9qSaGXFyg.

Bednarik, Roman, Tomi Kinnunen, Andrei Mihaila, and Pasi Fränti. 2005. "Eye-Movements as a Biometric." In *Image Analysis*, edited by Heikki Kalviainen, Jussi Parkkinen, and Arto Kaarna, 780–89. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/11499145_79.

Brunyé, Tad T., Trafton Drew, Donald L. Weaver, and Joann G. Elmore. 2019. "A Review of Eye Tracking for Understanding and Improving Diagnostic Interpretation." *Cognitive Research: Principles and Implications* 4 (1): 7. https://doi.org/10.1186/s41235-019-0159-2.

Carter, Benjamin T., and Steven G. Luke. 2020. "Best Practices in Eye Tracking Research." *International Journal of Psychophysiology* 155 (September): 49–62. https://doi.org/10.1016/j.ijpsycho.2020.05.010.

Chen, Jidong, and Yiqing Xu. 2017. "Information Manipulation and Reform in Authoritarian Regimes." *Political Science Research and Methods* 5 (1): 163–78. https://doi.org/10.1017/psrm.2015.21.

Chen, Ming Shin. 2019. "China's Data Collection on US Citizens: Implications, Risks, and Solutions" 15 (1).

Chennamma, H R, and Xiaohui Yuan. 2013. "A SURVEY ON EYE-GAZE TRACKING TECHNIQUES" 4.

Clutch. 2023. "Visual Camp Client Reviews." 2023. https://clutch.co/profile/visualcamp.

David-John, Brendan, Diane Hosfelt, Kevin Butler, and Eakta Jain. 2021. "A Privacy-Preserving Approach to Streaming Eye-Tracking Data." *IEEE Transactions on Visualization and Computer Graphics* 27 (5): 2555–65. https://doi.org/10.1109/TVCG.2021.3067787.

Daxecker, Franz. 1992. "Christoph Scheiner's Eye Studies." *Documenta Ophthalmologica* 81 (1): 27–35. https://doi.org/10.1007/BF00155011.

De Jesús, Rosales-Banderas José, López-Sánchez Máximo, Pinto-Elías Raúl, and González-Serna Gabriel. 2016. "Methodology for Iris Scanning through Smartphones." In *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, 861–64. https://doi.org/10.1109/CSCI.2016.0167.

Gans, Joshua, and Abhishek Nagaraj. 2023. "What Is Apple's Vision Pro Really For?" *Harvard Business Review*, June 14, 2023. https://hbr.org/2023/06/what-is-apples-vision-pro-really-for.

Gent, Edd. 2023. "A Cryptocurrency for the Masses or a Universal ID?: Worldcoin Aims to Scan All the World's Eyeballs." *IEEE Spectrum* 60 (1): 42–57.

Jin-young, Cho. 2016. “Visual Camp Selected as a 2016 Red Herring Top 100 Asia - Businesskorea.” August 25, 2016. https://www.businesskorea.co.kr/news/articleView.html?idxno=15643.

Kavusi, Hajar, Keivan Maghooli, and Siamak Haghipour. 2023. “A Novel and Smarter Model to Authenticate and Identify People Intelligently for Security Purposes.” *Telecommunication Systems* 82 (1): 27–43. https://doi.org/10.1007/s11235-022-00957-4.

Kostka, Genia, Léa Steinacker, and Miriam Meckel. 2021. “Between Security and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the United Kingdom, and the United States.” *Public Understanding of Science* 30 (6): 671–90. https://doi.org/10.1177/09636625211001555.

Kröger, Jacob Leon, Otto Hans-Martin Lutz, and Florian Müller. 2020. “What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking.” In *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers*, edited by Michael Friedewald, Melek Önen, Eva Lievens, Stephan Krenn, and Samuel Fricker, 226–41. IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-42504-3_15.

LaPira, Timothy, and Herschel F. Thomas III. 2017. *Revolving Door Lobbying: Public Service, Private Influence, and the Unequal Representation of Interests*. University Press of Kansas.

Liebling, Daniel J., and Sören Preibusch. 2014. “Privacy Considerations for a Pervasive Eye Tracking World.” In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, 1169–77. Seattle Washington: ACM. https://doi.org/10.1145/2638728.2641688.

Lyon, David. 2022. “Surveillance.” *Internet Policy Review* 11 (4). https://policyreview.info/concepts/surveillance.

Marinović, Dunja, Sanja Njirić, Miran Čoklo, and Vedrana Muzic. 2011. “Personal Identification by Eyes.” *Collegium Antropologicum* 35 Suppl 2 (September): 347–50.

Morimoto, Carlos H., and Marcio R. M. Mimica. 2005. “Eye Gaze Tracking Techniques for Interactive Applications.” *Computer Vision and Image Understanding*, Special Issue on Eye Detection and Tracking, 98 (1): 4–24. https://doi.org/10.1016/j.cviu.2004.07.010.

Odu, Tiwalade, and Francis Idachaba. 2011. *A Review of the Fingerprint, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technologies*.

OpenSecrets. 2023. “Lobbying Data Summary.” OpenSecrets. 2023. https://www.opensecrets.org/federal-lobbying.

Ould Mohamed, Abdallahi, Matthieu Perreira da Silva, and Vincent Courboulay. 2007. “A History of Eye Gaze Tracking.” https://hal.science/hal-00215967.

Punde, Pramodini A., Mukti E. Jadhav, and Ramesh R. Manza. 2017. “A Study of Eye Tracking Technology and Its Applications.” In *2017 1st International Conference on Intelligent Systems and Information Management (ICISIM)*, 86–90. https://doi.org/10.1109/ICISIM.2017.8122153.

Qiang, Xiao. 2019. “President Xi’s Surveillance State The Road to Digital Unfreedom.” *Journal of Democracy* 30 (1): 53–67.

Raphael, J. R. 2016. “Why Most People Won’t Use a Smartphone Iris Scanner (a La the Galaxy Note 7’s).” Computerworld. August 4, 2016. https://www.computerworld.com/article/3104113/iris-scanner-galaxy-note-7.html.

Roussi, Antoaneta. 2020. “Resisting the Rise of Facial Recognition.” *Nature* 587 (7834): 350–54. https://doi.org/10.1038/d41586-020-03188-2.

“Securing Authoritarian Capitalism in the Digital Age: The Political Economy of Surveillance in China.” n.d. Accessed August 11, 2023. https://doi.org/10.1086/720144.

Simon, Gérard. 1975. “14.3. On the Theory of Visual Perception of Kepler and Descartes: Reflections on the Role of Mechanism in the Birth of Modern Science.” *Vistas in Astronomy* 18 (January): 825–32. https://doi.org/10.1016/0083-6656(75)90174-9.

Venugopal, Divya, J Amudha, and C. Jyotsna. 2016. “Developing an Application Using Eye Tracker.” In *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 1518–22. https://doi.org/10.1109/RTEICT.2016.7808086.

VisualCamp, dir. 2020. *[VisualCamp] SeeSo SDK Introduction*. https://www.youtube.com/watch?v=jVeFFIZbia8.

———. 2023. “SeeSo::The Gaze Tracker.” SeeSo. 2023. https://seeso.io/.

Yang, Jae weon, Dowoo Kim, and Sungwon Jung. 2020. “Using Eye-Tracking Technology to Measure Environmental Factors Affecting Street Robbery Decision-Making in Virtual Environments.” *Sustainability* 12 (18): 7419. https://doi.org/10.3390/su12187419.

Zhang, Xucong, Yusuke Sugano, Mario Fritz, and Andreas Bulling. 2019. “MPIIGaze: Real-World Dataset and Deep Appearance-Based Gaze Estimation.” *IEEE Transactions on Pattern Analysis and Machine Intelligence* 41 (1): 162–75. https://doi.org/10.1109/TPAMI.2017.2778103.