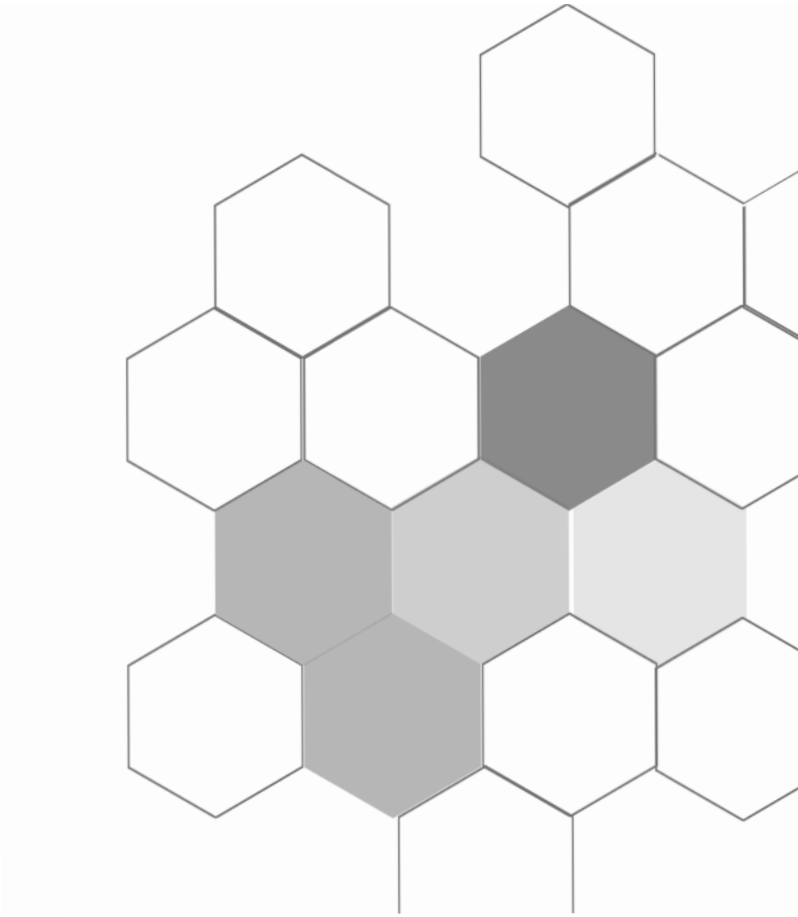
Ethical challenges in webcam eyetracking

V. 1
TAIMUR KHAN, ADSATA
JANUARY, 2022



1. Introduction

The world of UX analytics is thriving in the 21st century. As the global internet economy grows exponentially, digital businesses are relying on newer and better ways of reaching consumers. Online shops and services are becoming intelligent, learning from the behaviour of their users even before they land on their servers. This rise of an intelligent internet has caused visual information to become more personalised, making user experiences personalised as well. All this has driven the need for digital business to study the interaction of users with their products better, causing UX analytics tools to become synonymous with user-centred design and innovation. However, these tools are not always upholding standards deemed ethical.

At Adsata, we are building a browser-based exploratory data analysis tool for measuring visual interaction on the web. How, you may ask, can one measure visual interaction? We use complex AI in our browser based real-time webcam eyetracking software. This software allows users to:

1. create controlled online eyetracking studies for images and websites,
2. invite participants and collect eyetracking data,
3. explore the data metrics and visualisations calculated by the software to understand visual attention at individual and aggregated levels.

Since visual interaction makes up 98% of all user interactions with the web, naturally there were many ethical challenges for Adsata while building its software. Machine learning technologies used in webcam eyetracking tools present issues such as model bias, limited training data, data processing and so forth that can present ethical dilemmas. Naturally, the topics of biometric data collection also raises ethical considerations that are not only pertinent to ensure no misuse can happen, but also also to make sure humans are at the centre of any design related decisions made using eyetracking data. Therefore, ethical implications are also arising for researchers and practitioners using webcam eyetracking tools to remotely collect eyetracking data.

As webcam eyetracking becomes more accessible, researchers and practitioners face fundamentally new challenges regarding privacy and ethics. However, the topic of ethics in webcam eyetracking is fairly under-researched. An active discussion about ethical and social implications as well as issues of data privacy is important for the further development of webcam eyetracking technology and its acceptance in society.

In this paper, we aim to create a basic understanding of the reader in the issues of privacy and ethics in webcam eyetracking, as well as to raise awareness regarding how Adsata addresses such issues. The first part of the paper will summarise machine and data ethics to give a basic overview of the ethical and privacy issues arising from the technology driving webcam eyetracking tools. The second part will then discuss ethical and privacy challenges in eyetracking studies for the end users. Lastly, we will present how Adsata's software addresses the considerations raised in the first two parts.

We also want to highlight that the ethics of webcam eyetracking technology are often focused on "concerns" of various sorts,

which is a typical response to new technologies. Many such concerns turn out to be rather quaint; some are predictably wrong when they suggest that the technology is inherently unethical; but some concerns are broadly correct and deeply relevant. The task of a white paper such as this is to analyse the issues and to deflate the non-issues.

2. Ethical challenges

Advances in the research of machine[1] and data[2] ethics provide a firm basis for creating webcam eyetracking tools that address ethical challenges arising from technology.

Since most, if not all, modern webcam eyetracking tools use machine learning models in their software, therefore machine ethics become quite relevant to understanding the faults and biases arsing from the algorithms and training methods used in machine learning models.

Similarly, as sensitive data is involved at the data collection and processing steps, best-practices in data ethics research provide a foundation for solutions to concerns arising from webcam eyetracking.

Let's take a look at a few aspects that create ethical and privacy concerns in webcam eyetracking.

2.1 Algorithms, facial recognition, and model fairness

Model fairness refers to the various attempts at correcting algorithmic bias. While definitions of fairness are constantly researched, results may be considered fair if they are independent of given variables, especially those considered sensitive, such as the traits of individuals that should not correlate with the outcome (i.e. gender, ethnicity, sexual orientation, disability, etc.).

A core component of any webcam eyetracking software is facial recognition. It seems intuitive that eyetracking software needs to be aware of the participant's face in order to be able to predict where they are looking on the screen. Most modern webcam eyetracking software implementations use machine learning models in computer vision for facial recognition, which output computationally efficient and more accurate facial coding data. However, facial recognition models can present model bias in various ways.

For example, Buolamwini et al, 2018 analysed the accuracy of commercial gender classification products across light and dark skinned males and females. Their research considered products sold by Microsoft, Face++ and IBM and found them to perform far better on males and light skinned people — Table 1 shows each product's accuracy in predicting a binary classification of male or female from an image.

[1] **Machine ethics** is a part of the ethics of artificial intelligence (AI) and machine learning (ML) concerned with adding or ensuring moral behaviours of human-made machines that use AI/ML.

[2] **Data ethics** encompasses the moral obligations of gathering, protecting, and using personally identifiable information and how it affects individuals.

	Microsoft	*Face++*	*IBM*
Dark Skinned Female	20.8%	34.5%	34.7%
Light Skinned Female	1.7%	6.0%	7.1%
Dark Skinned Male	6.0%	0.7%	12.0%
Light Skinned Male	0.0%	0.8%	0.3%

Table 1. Error rates in commercial facial coding based gender classification products (Buolamwini et al, 2018).

Similarly, a recent study titled "Face Recognition: Too Bias, or Not Too Bias" [3] showed a skew in performance for minority demographics (e.g., Asian Females and Indian Males), and a clear percent difference for the majority (e.g., White Males and White Females) when training a machine learning model.

Although machine learning based webcam eyetracking approaches do not usually rely on classification models, such studies do show an inherent bias in the way these models interpret human facial features. And since facial coding models are part of the webcam eyetracking process, any such bias left unchecked will cause the data to inherit the bias as well.

2.2 Data collection and processing

Gaze data is unique as it differs from other signals of human activity. We can disguise our voices to fool speech recognisers; alter our appearances with clothing and makeup, and change our keystrokes to defeat key-loggers; however, we have only partial control of our gaze. This uniqueness of gaze data also demands unique ways of collecting and processing such data in order to ensure participant's data privacy.

One of the key issues with webcam eyetracking data in particular is the need to process video data from the webcam. Traditional webcam eyetracking approaches involved recording and sending the webcam feeds of participants to remote servers for processing. Such an approach was seen with one of the first webcam eyetracking tools called GazeHawk. Although server-side processing of the webcam feeds has its merits, it also creates a point of data privacy concern for the participants.

The gaze data that is collected through server-side processing approaches results in privacy losses of two kinds: first, the identity of an individual and second, the inference of interests of the individual. The leakage of information about identity and interests violates the privacy principle of informational self-determination. There is a twofold loss in users' ability to determine for themselves when, how, and to what extent information about them is communicated to others.

2.3 Data transparency

In order to give the participants their right of self-determination, it is pertinent to ensure transparency regarding the data collected from them. This is not only required by data privacy regulations like the General Data Privacy Regulation (GDPR) and California Consumer Privacy Act (CCPA), but it also creates trust between the creators of webcam eyetracking studies and its participants.

One of the key challenges in webcam eyetracking studies is the difficulty to persuade unknown individuals online to

participate in such studies. A lack of transparency in not only what type of data is collected, but also of how the data is processed can exacerbate this issue of participant recruitment.

The webcam eyetracking community should begin to consider data transparency in webcam eyetracking systems as they become more pervasive. It is unreasonable to expect a user to understand the mapping of raw data to sensitive attributes. Instead, it is up to the developers to inform the user in a comprehensible way about the data being collected and its potential implications, and let the user limit the data in sensible ways.

Although technology plays a large part in the ethical challenges faced by webcam eyetracking systems, there is also a concern of ethical challenges presented for the users using these tools to create eyetracking studies. Let's take a look at the few ways in which ethical challenges can arise from creating eyetracking studies.

2.4 Participant anonymity

In the context of webcam eyetracking, eyetracking studies can essentially be thought of as online surveys. It goes without saying that the anonymity, confidentiality and security of participant data has to be the top priority when conducting online surveys. According to article 6 of the GDPR, you need a lawful basis before you can process personal data so that the participant is able to choose what happens to their data. This, again, ensures the right of self-determination.

A concern with frameworks like GDPR is that some times they can be too broad to cover specific cases. In the case of online surveys, If you conduct a survey anonymously – without referring to personal data – GDPR does not apply. However, the term anonymous is quite vague. How can a participant be sure a survey is truly anonymous? In fact, even if a survey does not collect personal details from participants (such as their name, email address, etc.) it does not mean that the survey is truly anonymous. If data can be traced back to the survey participants in any way, then the survey is personalised.

Therefore, it is not enough to simply mention survey anonymisation in communication; the necessary technical and organisational framework must also be established. Aspects like the **SSL encryption** of data and the technical **security of survey servers** play a major role in this regard.

2.5 Study and stimulus selection

At its core, eye movement data is usually coded as (x, y, time) tuples/objects. Depending on the eyetracker, pupil dilation may also be reported. This time series data is noisy due to biological noise arising from movement, as well as from ambient conditions and sensor uncertainty[3]. In many applications, eye movements are condensed into fixations that approximate the focus of attention. Ordered in time, the sequence of fixations sequence comprises a scanpath. Such data may be coupled with details about the underlying stimuli (e.g., areas of interest displayed on screen), creating a richer notion of both what was attended to and how attention varied. Even without knowledge of the stimuli, some

[3] The sensor uncertainty (or probable error of measurement) is also called the **95% uncertainty**. In technical terms, it is the two standard deviations or 2σ (two sigma) variation.

scanpaths are highly stereotyped and recognisable. Knowing how and certainly at what people gaze provides a wealth of understanding. Yet gaze data intended for a single purpose such as evaluating a new user interface can unwittingly reveal sensitive attributes of participants when it is analysed more deeply.

2.6 Consensual studies

The GDPR has very clear requirements when it comes to the consent to collect personal data of online survey participants which, as we have established, also apply to webcam eyetracking studies.

According to GDPR, the consent of the participants is **ONLY** effective if the stipulated conditions are met. The online survey needs to include a section where it clearly informs the participants about how the collected personal data will be used and the purpose of the survey. Data collection without the prior consent of the participant is strictly forbidden.

3. Adsata's approach

3.1 Technology

Adsata software uses modern edge machine learning methods to achieve its end goal of webcam eyetracking. Adsata relies on modified versions of the open source softwares called Webgazer and MediaPipes's Face Mesh library for creating facial coding data and predicting gaze movements based on this data in real time.

Although the complete technical details of how gaze movements are predicted by the combination of these two softwares is beyond the scope of this white paper, the steps involved have been broken down below to give the reader a general sense.

Before diving into the explanation of the process, it is absolutely necessary to understand that Adsata's software processes all facial coding data and generates eyetracking predictions in real-time: **meaning the facial coding data and the webcam feed never leave the browser environment.**

Here are the steps:

1. The webcam video feed is processed as individual images at an optimised frame rate. Let's take a single image as an example.

Figure 1. An example image to demonstrate a single frame of a webcam feed.

2. The Face Mesh library is then used to detect and encode 468 facial landmarks. The images from the landmarks for the eyes of the participant are cut out (Figure 2).

Figure 2. The eyes as the are detected by the Face Mesh. facial coding data

3. The data from the eyes of the participant is then scaled down for the purpose of computational efficiency, is converted to greyscale, and the greyscale images are normalised (Figure 3).

Figure 3. Eye data is scaled down (1), then converted to greyscale (2), and then the greyscale image is normalised (3).

4. The grey value between 0 and 255 of each pixel in the scaled and normalised greyscale datapoints are determined in 10x6 matrices (Table 2).

Left

132	84	60	30	79	118	110	96	106	161
101	42	46	44	48	143	96	17	116	117
16	57	118	43	31	37	39	46	123	118
59	153	211	134	95	72	86	198	96	189
85	158	214	180	125	120	216	224	200	91
159	112	96	116	141	175	197	179	208	213

Right

127	170	171	162	136	100	93	86	110	152
174	171	114	178	74	82	54	47	62	141
178	114	93	83	33	9	8	9	61	13
172	78	126	219	120	76	97	119	189	104
175	192	194	226	222	124	133	189	184	94
190	196	166	158	151	185	133	135	153	163

Table 2. The tables above show the matrix of RGB values for each pixel in normalised greyscale images for each eye. The order of the pixels in determined by the position in the table

5. The pixel RGB values are then processed by Webgazer to determine the position of the eye while looking at something on the screen. These processed values are x,y coordinates on the screen and timestamps (Figure 4).

```
1 {x: 532, y: 712, timestamp: 1203}
```

Figure 4. A single Webgazer prediction of what the participant is looking at a given point in time.

6. As the study ends, all the predictions are sent from the browser to Adsata's database. No facial coding data, or images leave the browser, but simply a list of x,y coordinates and timestamps.

3.2 Addressing ethical challenges

Adsata's approach to webcam eyetracking addresses the ethical challenges outlined earlier in this paper.

Algorithms, facial recognition, and model fairness: The facial coding model (Face Mesh) used by Adsata was originally developed by engineers at Google [2]. The creators of the model performed a thorough fairness evaluation based on Google's Ethical Artificial Intelligence principles.

For this purpose, a training dataset for the Face Mesh model was created using 1700 samples evenly distributed across 17 geographical subregions (Figure 5)[2]. Therefore, each region contains 100 images.

Furthermore, a detailed "fairness" analysis was done by cross checking the dataset with a human annotated dataset to evaluate model bias across genders and skin tones in the training dataset.

Results of the fairness analysis for Face Mesh showed a Mean Absolute Error of

2.77% across genders and 2.69% across skin tones [2].

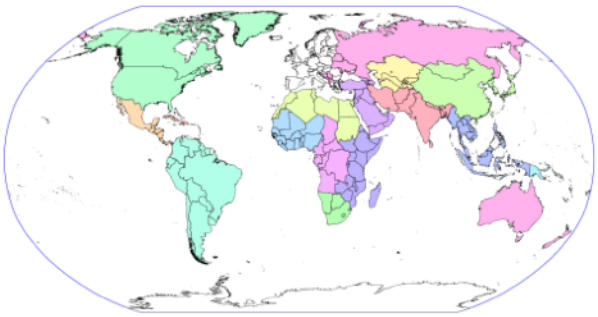


Figure 5. Samples for the training data of the Face Mesh were taken from 17 different subregions of the world Eat unique colour represents a specific subregion [3].

Participant anonymity, Data collection & processing: Due to Adsata's use of edge Machine Learning methods, Adsata's system ensures that no personally identifiable information of the participants ever leaves the browser. This includes not only obvious data points like facial coding data and webcam feed, but also hidden points like participant's IP addresses and geolocation. Additionally, client and server side methods in data validation and sanitisation are also deployed to safeguard Adsata and the participants of its webcam eyetracking studies from cross-site scripting and other vector attacks.

Data transparency + participant consent: Participants in Adsata's eyetracking studies are required to read through Adsata's Data Privacy Agreement and give explicit consent before participating in eyetracking studies. Eyetracking studies also cannot be created without the participant's consent and awareness (e.g. through code injection). It is then the participant's choice whether to participate or not. Therefore, the consent check box cannot be pre-ticked and the participants need to tick it themselves. These measures make Adsata's system completely GDPR compliant.

Study and stimulus selection: Although this is more of a technological barrier rather than an active choice, Adsata's system is not capable of detecting changes in participants' pupil sizes. This makes it impossible to predict any physical or demographic attributes of the participants purely through their pupil data.

4. The way forward

With the onset of technological advancements, it is clear that webcam eyetracking systems present a promising alternative to in-lab eyetracking hardware. Although webcam eyetracking systems have technological restrictions in terms of data quality, advancements in browser-based technologies (e.g. Tensorflow.js and WebAssembly) continue to improve such systems. Such technologies present reliable browser-based computational tools to process large amounts of data, but also ensure that participant data is in the most secure environment: their own devices.

It is also clear that webcam eyetracking technologies raise their own set of ethical challenges for the creators of the tool and the users. Many of these ethical challenges can be overcome with newer technology, however some of these challenges depend on how professionals use such tools. In a way, it matters who is behind the lens, who is tracking the eyes, and what they are they studying. As humans continue to evolve the virtual space, the question of how we collect and use human interaction data to improve visual systems has never been more relevant.

The affordable prices and scalability of webcam eyetracking devices, combined with the maturity of analytical methods, have made gaze data a standard source of information when studying human-computer interaction, user behaviour or cognition. An extensive debate between all stakeholders on how to approach webcam eyetracking is still lacking and we hope this white paper will help open such a discussion.

References

[1] Buolamwini, Joy, and Timnit Gebru. "Gender shades: Intersectional accuracy disparities in commercial gender classification." *Conference on fairness, accountability and transparency*. PMLR, 2018.

[2] Kartynnik, Yury, et al. "Real-time facial surface geometry from monocular video on mobile GPUs." *arXiv preprint arXiv:1907.06724* (2019).

[3] Robinson, Joseph P., et al. "Face recognition: too bias, or not too bias?." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. 2020.