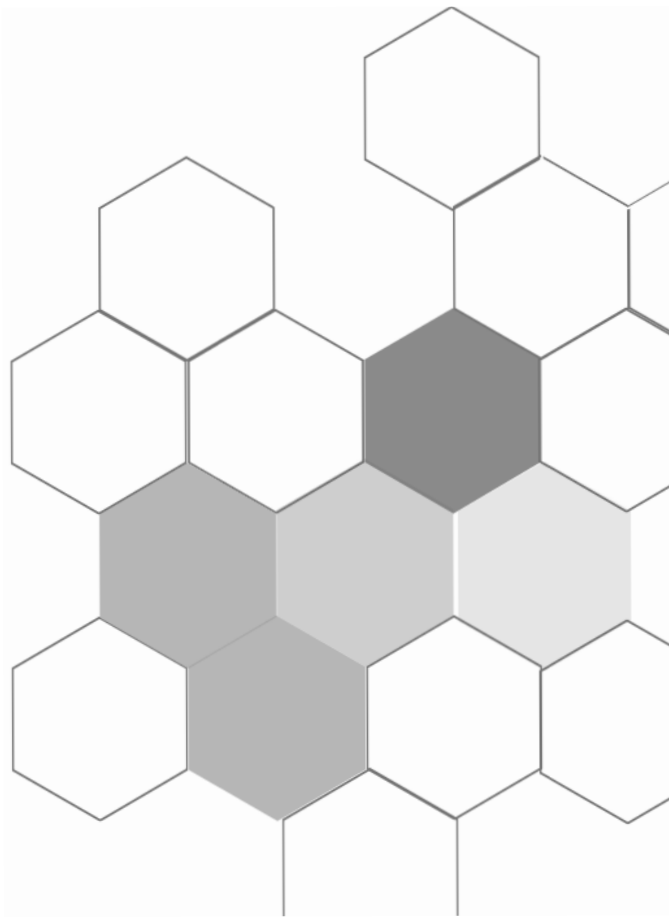
Ethische Herausforderungen bei Webcam-Eyetracking

V. 1
TAIMUR KHAN, ADSATA
JANUARY, 2022



1. Einleitung

Die Welt der UX-Anylytics entwickelt sich im 21. Jahrhundert rasant. Mit dem exponentiellen Wachstum der globalen Internetwirtschaft verlassen sich digitale Unternehmen auf neue und bessere Wege, um die Verbraucher zu erreichen. Online-Shops und -Dienste werden immer intelligenter und lernen aus dem Verhalten ihrer Nutzer, noch bevor diese ihre Produkte nutzen. Das Aufkommen eines intelligenten Internets hat dazu geführt, dass visuelle Informationen immer stärker personalisiert werdenund damit auch die Nutzererfahrung. All dies hat zur Folge, dass digitale Unternehmen die Interaktion von Nutzern mit ihren Produkten besser untersuchen müssen; damit werdenUX-Analysetools zum Synonym für nutzerzentriertes Design und Innovation. Allerdings halten diese Tools nicht immer die als ethisch angesehenen Standards ein.

Mit Adsata entwickeln wir ein browserbasiertes, exploratives Datenanalysetool zur Messung visueller Interaktion im Web. Wie wir visuelle Interaktion messen? Wir verwenden komplexe KI in unserer browserbasierten Echtzeit-Webcam-Eyetracking-Software. Diese Software ermöglicht es den Benutzern:

1. kontrollierte Online-Eyetracking-Studien für Bilder und Websites zu erstellen,

2. Teilnehmer einzuladen und Eyetracking-Daten zu sammeln,

3. die von der Software ermittelten Daten, Metriken und Visualisierungen zu untersuchen, um die visuelle Aufmerksamkeit auf individueller und aggregierter Ebene zu verstehen.

Da die visuelle Interaktion 98 % aller Nutzerinteraktionen im Internet ausmacht, gab es für Adsata bei der Entwicklung seiner Software viele ethische Herausforderungen. Die Technologien des maschinellen Lernens, die in den Tools für das Eyetracking per Webcam verwendet werden, werfen Probleme auf, wie z. B. die Verzerrung des Modells, begrenzte Trainingsdaten, Datenverarbeitung usw., die zu ethischen Dilemmata führen können.

Natürlich wirft das Thema der biometrischen Datenerfassung auch ethische Überlegungen auf, die nicht nur relevant sind, um sicherzustellen, dass kein Missbrauch stattfindet, sondern auch, um zu gewährleisten, dass der Mensch im Mittelpunkt aller Designentscheidungen steht, die auf Basis von Eyetracking-Daten getroffen werden. Daher ergeben sich auch ethische Implikationen für Forscher und Praktiker, die Webcam-Eyetracking-Tools verwenden, um Eyetracking-Daten remotezu erfassen.

In dem Maße, in dem Webcam-Eyetracking immer zugänglicher wird, stehen Forscher und Praktiker vor grundlegend neuen Herausforderungen in Bezug auf Datenschutz und Ethik. Das Thema Ethik beim Webcam-Eyetracking ist jedoch noch relativ wenig erforscht. Eine aktive Diskussion über ethische und soziale Implikationen sowie Fragen des Datenschutzes ist wichtig für die weitere Entwicklung der Webcam-Eyetracking-Technologie und ihre Akzeptanz in der Gesellschaft.

In diesem Beitrag möchten wir dem Leser ein grundlegendes Verständnis für die Fragen des Datenschutzes und der Ethik beim Webcam-Eyetracking vermitteln und das Bewusstsein dafür schärfen, wie Adsata mit diesen Fragen umgeht. Der

erste Teil fasst dazu Maschinen- und Datenethik zusammen, um einen grundlegenden Überblick über die ethischen und datenschutzrechtlichen Fragen zu geben, die sich aus der Technologie von Webcam-Eyetracking-Tools ergeben. Im zweiten Teil werden dann die ethischen und datenschutzrechtlichen Herausforderungen bei Eyetracking-Studien für die Endnutzer erörtert. Abschließend werden wir darlegen, wie die Software von Adsata die in den ersten beiden Teilen aufgeworfenen Überlegungen berücksichtigt.

Wir möchten auch darauf hinweisen, dass die Ethik der Webcam-Eyetracking-Technologie sich oft auf "Bedenken" verschiedener Art konzentriert, was eine typische Reaktion auf neue Technologien ist. Viele dieser Bedenken erweisen sich als eher kurios; einige sind offensichtlich falsch wenn sie etwa darauf hindeuten, dass die Technologie von Natur aus unethisch ist; aber einige Bedenken sind durchaus richtig und sehr relevant. Die Aufgabe dieses Whitepapers besteht darin, die Probleme zu analysieren und die Nicht-Probleme zu entkräften.

2. Ethische Herausforderungen

Die Fortschritte in der Forschung auf dem Gebiet der Maschinen- und Datenethik bieten eine solide Grundlage für die Entwicklung von Webcam-Eyetracking-Tools, die sich mit den ethischen Herausforderungen befassen, die sich aus der Technologie ergeben.
Da die meisten, wenn nicht sogar alle, modernen Webcam-Eyetracking-Tools maschinelle Lernmodelle in ihrer Software verwenden, ist die Maschinenethik von großer Bedeutung für das Verständnis der Fehler und Verzerrungen, die sich aus den Algorithmen und Trainingsmethoden der maschinellen Lernmodelle ergeben.

Da es bei der Datenerfassung und -verarbeitung um sensible Daten geht, bieten die bewährten Praktiken der Datenethikforschung eine Grundlage für die Lösung von Problemen, die durch das Eyetracking per Webcam entstehen.
Werfen wir also einen Blick auf einige Aspekte, die beim Webcam-Eyetracking ethische und datenschutzrechtliche Bedenken aufwerfen.

2.1 Algorithmen, Gesichtserkennung und ‚model fairness'

Model fairness bezieht sich auf die verschiedenen Versuche, algorithmische Verzerrungen zu korrigieren. Während Definitionen von Fairness variieren, können Ergebnisse generell als fair angesehen werden, wenn sie unabhängig von bestimmten Variablen sind, insbesondere von solchen, die als sensibel angesehen werden, wie z. B. die Eigenschaften von Personen, die nicht mit dem Ergebnis korrelieren sollten (z. B. Geschlecht, ethnische Zugehörigkeit, sexuelle Orientierung, Behinderung usw.).

Eine Kernkomponente jeder Webcam-Eyetracking-Software ist die Gesichtserkennung. Es erscheint intuitiv, dass die Eyetracking-Software das Gesicht des Teilnehmers kennen muss, um vorhersagen zu können, wohin der Teilnehmer auf dem Bildschirm schaut. Die meisten modernen Implementierungen von Eyetracking-Software für Webcams verwenden für die Gesichtserkennung maschinelle Lernmodelle aus dem Bereich der Computer-Vision, die rechnerisch effizientere und genauere Gesichtscodierungsdaten liefern. Gesichtserkennungsmodelle können

jedoch auf verschiedene Weise Modellverzerrungen aufweisen.

Buolamwini et al. (2018) analysierte beispielsweise die Genauigkeit kommerzieller Produkte zur Geschlechtsklassifizierung bei hell- und dunkelhäutigen Männern und Frauen. Die Studie untersuchte Produkte von Microsoft, Face++ und IBM und stellte fest, dass diese bei Männern und hellhäutigen Menschen deutlich besser abschneiden - Tabelle 1 zeigt die Genauigkeit der einzelnen Produkte bei der Vorhersage einer binären Klassifizierung von männlich oder weiblich anhand eines Bildes.

	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%

Tabelle 1. Fehlerquoten kommerzieller Produkte zur Geschlechtsklassifizierung durch Gesichtscodierung (Buolamwini et al., 2018).

Ähnlich verhält es sich mit einer aktuellen Studie mit dem Titel "Face Recognition: Too Bias, or Not Too Bias" [3]. Diese zeigte beim Training eines maschinellen Lernmodells eine verzerrte Leistung für Minderheiten (z. B. weibliche Asiatinnen und männliche Inder) und einen deutlichen prozentualen Unterschied für die Mehrheit (z. B. männliche und weibliche Weiße).

Obwohl auf maschinellem Lernen basierende Webcam-Eyetracking-Ansätze normalerweise nicht auf Klassifizierungsmodellen beruhen, zeigen solche Studien eine inhärente Verzerrung in der Art und Weise, wie diese Modelle menschliche Gesichtsmerkmale interpretieren. Und da Gesichtscodierungsmodelle Teil des Webcam-Eyetracking-Prozesses sind, führt jede unkontrollierte Verzerrung dazu, dass die Daten diese Verzerrung ebenfalls beinhalten.

2.2 Datenerfassung und -verarbeitung

Blickdaten sind einzigartig, da sie sich von anderen Signalen menschlicher Aktivität unterscheiden. Wir können unsere Stimme verstellen, um Spracherkennungssoftware zu täuschen, unser Äußeres durch Kleidung und Make-up verändern und unsere Tastenanschläge ändern, um Key-Logger zu überlisten - aber wir haben nur teilweise Kontrolle über unseren Blick. Diese Einzigartigkeit der Blickdaten erfordert auch einzigartige Methoden zur Erfassung und Verarbeitung solcher Daten, um den Datenschutz der Teilnehmer zu gewährleisten.

Eines der Hauptprobleme bei Webcam-Eyetracking-Daten ist die Notwendigkeit, Videoaufzeichnungen der Webcam zu verarbeiten. Bei herkömmlichen Ansätzen zum Webcam-Eyetracking wurden die Webcam-Bilder der Teilnehmer aufgezeichnet und zur Verarbeitung an weit entfernte Server gesendet. Ein solcher Ansatz wurde mit einem der ersten Webcam-Eyetracking-Tools namens GazeHawk verfolgt. Die serverseitige Verarbeitung der Webcam-Feeds hat zwar ihre Vorzüge, stellt aber auch ein Problem für den Datenschutz der Teilnehmer dar.

Die Blickdaten, die durch serverseitige Verarbeitungsansätze gesammelt werden, führen zu einem Verlust der Privatsphäre in zweierlei Hinsicht: erstens der Identität einer Person und zweitens der Rückschlüsse auf die Interessen der Person. Das Durchsickern von Informationen über Identität und Interessen verstößt gegen das Prinzip der informationellen Selbstbestimmung. Die Nutzer verlieren in zweifacher Hinsicht die Möglichkeit, selbst zu bestimmen wann, wie und in welchem Umfang Informationen über sie an andere weitergegeben werden.

2.3 Transparenz der Daten

Um den Teilnehmern ihr Selbstbestimmungsrecht zu gewähren, ist es wichtig, Transparenz über die von ihnen erhobenen Daten zu gewährleisten. Dies ist nicht nur aufgrund von Datenschutzbestimmungen wie der Datenschutz-Grundverordnung (DSGVO) und dem California Consumer Privacy Act (CCPA) erforderlich, sondern schafft auch Vertrauen zwischen den Urhebern von Webcam-Eyetracking-Studien und den Teilnehmern.

Eine der größten Herausforderungen bei Webcam-Eyetracking-Studien ist die Schwierigkeit, unbekannte Personen online zur Teilnahme an solchen Studien zu überreden. Mangelnde Transparenz nicht nur in Bezug auf die Art der erhobenen Daten, sondern auch in Bezug auf die Verarbeitung der Daten kann das Problem der Teilnehmerrekrutierung noch verschärfen.

Die wachsende Webcam-Eyetracking-Community sollte dementsprechend die Datentransparenz bei Webcam-Eyetracking-Systemen stärker berücksichtigen. Es ist unzumutbar, von einem Benutzer zu erwarten, dass er die Zuordnung von Rohdaten zu sensiblen Attributen versteht. Stattdessen ist es Aufgabe der Entwickler, den Benutzer auf verständliche Weise über die gesammelten Daten und ihre möglichen Auswirkungen zu informieren und ihm die Möglichkeit zu geben, die Daten auf sinnvolle Weise zu begrenzen.

Neben den technischen Tools selbst ergeben sich ethische Herausforderungen auch auf Seiten der Nutzer, die diese Tools zur Erstellung von Eyetracking-Studien verwenden. Werfen wir einen Blick auf einige Möglichkeiten, wie ethische Herausforderungen bei der Erstellung von Eyetracking-Studien entstehen können.

2.4 Anonymität der Teilnehmer

Im Zusammenhang mit Webcam-Eyetracking können Eyetracking-Studien im Wesentlichen als Online-Umfragen betrachtet werden. Anonymität, Vertraulichkeit und Sicherheit der Teilnehmerdaten müssen grundsätzlich bei der Durchführung von Online-Umfragen oberste Priorität haben. Gemäß Artikel 6 der Datenschutz-Grundverordnung (DSGVO) ist für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage erforderlich, damit die Teilnehmer selbst entscheiden können, was mit ihren Daten geschieht. Dies wiederum gewährleistet das Recht auf Selbstbestimmung.

Ein Problem mit Rahmenregelungen wie der DSGVO ist, dass sie manchmal zu weit gefasst sein können, um bestimmte Fälle abzudecken. Im Falle von Online-Umfragen gilt die Datenschutz-Grundverordnung nicht, wenn Sie eine Umfrage anonym durchführen - ohne Bezug auf

personenbezogene Daten. Der Begriff "anonym" ist jedoch recht vage. Wie kann ein Teilnehmer sicher sein, dass eine Umfrage wirklich anonym ist? Selbst wenn bei einer Umfrage keine personenbezogenen Daten von den Teilnehmern erhoben werden (z. B. ihr Name, ihre E-Mail-Adresse usw.), bedeutet dies nicht, dass die Umfrage wirklich anonym ist. Wenn die Daten in irgendeiner Weise zu den Umfrageteilnehmern zurückverfolgt werden können, dann ist die Umfrage personalisiert.

Daher reicht es nicht aus, in der Kommunikation nur die Anonymisierung der Umfrage zu erwähnen, sondern es müssen auch die notwendigen technischen und organisatorischen Rahmenbedingungen geschaffen werden. Aspekte wie die **SSL-Verschlüsselung** der Daten und die technische **Sicherheit der Befragungsserver** spielen dabei eine große Rolle.

2.5 Studien- und Stimulusauswahl

Augenbewegungsdaten sind im Kern meist als (x, y, Zeit) Tupel/Objekte codiert. Je nach Eyetracker kann auch die Pupillenerweiterung erfasst werden. Diese Zeitreihendaten sind aufgrund des biologischen Rauschens, das durch die Bewegung entsteht, sowie aufgrund der Umgebungsbedingungen und der Unsicherheit des Sensors ‚verrauscht'. In vielen Anwendungen werden die Augenbewegungen zu Fixationen verdichtet, die dem Fokus der Aufmerksamkeit entsprechen. Die zeitlich geordnete Abfolge von Fixationen umfasst einen Scan-Pfad. Solche Daten können mit Details über die zugrundeliegenden Stimuli (z. B. die auf dem Bildschirm angezeigten Bereiche von Interesse) gekoppelt werden, wodurch eine umfassendere Vorstellung davon entsteht, worauf die Aufmerksamkeit gerichtet war und wie sie variierte. Auch ohne Kenntnis der Stimuli sind einige Scanpfade sehr stereotyp und wiedererkennbar. Wenn man weiß, wie und worauf Menschen blicken, erhält man eine Fülle von Informationen. Doch Blickdaten, die für einen einzigen Zweck bestimmt sind, z. B. für die Bewertung einer neuen Benutzeroberfläche, können bei einer tieferen Analyse ungewollt sensible Eigenschaften der Teilnehmer offenbaren.

2.6 Einvernehmliche Studien

Die Datenschutz-Grundverordnung (DSGVO) stellt sehr klare Anforderungen an die Einwilligung zur Erhebung personenbezogener Daten von Teilnehmern an Online-Umfragen, die, wie wir festgestellt haben, auch für Studien mit Webcam-Eyetracking gelten.

Nach der GDPR ist die Einwilligung der Teilnehmer **NUR** dann wirksam, wenn die festgelegten Bedingungen auch erfüllt sind. Die Online-Umfrage muss einen Abschnitt enthalten, in dem die Teilnehmer eindeutig darüber informiert werden, wie die erhobenen personenbezogenen Daten verwendet werden und welchen Zweck die Umfrage hat. Die Datenerhebung ohne die vorherige Zustimmung des Teilnehmers ist strengstens untersagt.

3. Der Ansatz von Adsata

3.1 Technologie

Die Adsata-Software nutzt moderne Methoden des maschinellen Lernens, um Webcam-Eyetracking-Daten zu erheben. Adsata stützt sich auf modifizierte Versionen der Open-Source-Software **‚Webgazer'** und der **„FaceMesh"** von

‚MediaPipes', um Gesichtscodierungsdaten zu erstellen und auf der Grundlage dieser Daten Blickbewegungen in Echtzeit vorherzusagen.

Obwohl die vollständigen technischen Details der Vorhersage von Blickbewegungen durch die Kombination dieser beiden Softwares den Rahmen dieses Whitepapers übersteigen würden, werden die beteiligten Schritte im Folgenden aufgeschlüsselt, um dem Leser einen allgemeinen Eindruck zu vermitteln.

Bevor wir in die Erklärung des Prozesses eintauchen, ist es notwendig zu verstehen, dass die Software von Adsata alle Gesichtscodierungsdaten verarbeitet und Eyetracking-Vorhersagen in Echtzeit generiert: Das bedeutet, dass die Gesichtscodierungsdaten und der Webcam-Feed die Browserumgebung und damit das Endgerät der Teilnehmer nie verlassen.

Der Ablauf Schritt für Schritt:

1. Das Webcam-Video wird in Einzelbildern mit einer optimierten Bildrate verarbeitet. Nehmen wir ein einzelnes Bild als Beispiel.

Abbildung 1. Ein Beispielbild zur Veranschaulichung eines Einzelbildes einer Webcam-Übertragung.

2. Die Face Mesh-Bibliothek wird dann zur Erkennung und Codierung von 468 Gesichtsmerkmalen verwendet. Die Bilder der Landmarken für die Augen des Teilnehmers werden ausgeschnitten (Abbildung 2).

Abbildung 2. Das Auge, wie es von den Face Mesh-Codierungsdaten erkannt wird.

3. Die Daten von den Augen des Teilnehmers werden dann zum Zweck der Recheneffizienz verkleinert, in Graustufen umgewandelt und die Graustufenbilder normalisiert (Abbildung 3).

4. Die Grauwerte zwischen 0 und 255 jedes

Abbildung 3. Die Augendaten werden verkleinert (1), dann in Graustufen umgewandelt (2), und anschließend wird das Graustufenbild normalisiert (3).

Pixels in den skalierten und normalisierten Graustufen-Datenpunkten werden in 10x6-Matrizen bestimmt (Tabelle 2).

Links

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

Rechts

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

Tabelle 2. Die obigen Tabellen zeigen die Matrix der RGB-Werte für jedes Pixel in normalisierten Graustufenbildern für jedes Auge. Die Reihenfolge der Pixel wird durch die Position in der Tabelle bestimmt.

5. Die Pixel-RGB-Werte werden dann von Webgazer verarbeitet, um die Position des Auges beim Betrachten von Inhalten auf dem Bildschirm zu bestimmen. Diese verarbeiteten Werte sind x,y-Koordinaten auf dem Bildschirm und Zeitstempel (Abbildung 4).

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

Abbildung 4. Eine einzelne Webgazer-Vorhersage dessen, was der Teilnehmer zu einem bestimmten

6. Am Ende der Studie werden alle Vorhersagen vom Browser an die Datenbank von Adsata gesendet. Keine Gesichtscodierungsdaten oder Bilder verlassen den Browser, sondern lediglich eine Liste von x,y-Koordinaten und Zeitstempeln

3.2 Umgang mit ethischen Herausforderungen

Adsatas Ansatz für das Webcam-Eyetracking geht auf die ethischen Herausforderungen ein, die weiter oben in diesem Dokument beschrieben wurden.

Algorithmen, Gesichtserkennung und Modellgerechtigkeit: Das von Adsata verwendete Gesichtscodierungsmodell (Face Mesh) wurde ursprünglich von Ingenieuren bei Google entwickelt [2]. Die Schöpfer des Modells führten eine ausführliche Fairness-Evaluierung durch, die auf den Grundsätzen der ethischen künstlichen Intelligenz von Google basiert.

Zu diesem Zweck wurde ein Trainingsdatensatz für das Face Mesh-Modell erstellt, der 1700 Proben enthält, die gleichmäßig auf 17 geografische Unterregionen verteilt sind (Abbildung 5) [2]. Jede Region enthält also 100 Bilder.

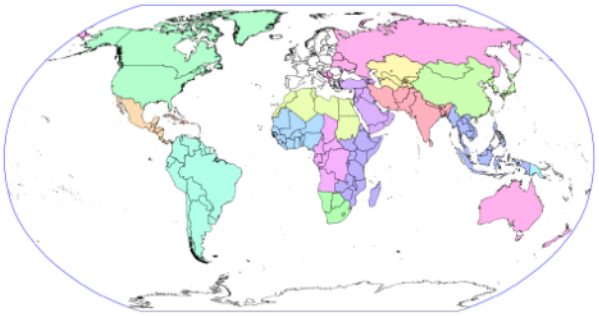


Abbildung 5. Die Stichproben für die Trainingsdaten des Gesichtsnetzes stammen aus 17 verschiedenen Unterregionen der Welt. Jede einzelne Farbe steht für

Darüber hinaus wurde eine detaillierte "Fairness"-Analyse durchgeführt, indem der Datensatz mit einem von Menschen kommentierten Datensatz abgeglichen wurde, um die Verzerrung des Modells bei verschiedenen Geschlechtern und Hautfarben im Trainingsdatensatz zu bewerten.

Die Ergebnisse der Fairness-Analyse für Face Mesh zeigten einen mittleren absoluten Fehler von 2,77 % für alle Geschlechter und 2,69 % für alle Hautfarben [2].

Anonymität der Teilnehmer, Datenerhebung und -verarbeitung: Durch die Verwendung von Edge-Machine-Learning-Methoden stellt das System von Adsata sicher, dass keine persönlich identifizierbaren Informationen der Teilnehmer jemals den Browser verlassen. Dazu gehören nicht nur offensichtliche Datenpunkte wie Gesichtscodierungsdaten und Webcam-Feed, sondern auch versteckte Punkte wie die IP-Adressen und Geolocation der Teilnehmer. Zusätzlich werden client- und serverseitige Methoden zur Datenvalidierung und -Bereinigung eingesetzt, um Adsata und die Teilnehmer seiner Webcam-Eyetracking-Studien vor Cross-Site-Scripting und anderen Vektorangriffen zu schützen.

Datentransparenz und Einwilligung der Teilnehmer: Die Teilnehmer an Adsatas Eyetracking-Studien müssen die Datenschutzvereinbarung von Adsata lesen und ihre ausdrückliche Zustimmung geben, bevor sie an Eyetracking-Studien teilnehmen. Eyetracking-Studien können auch nicht ohne die Zustimmung und das Wissen des Teilnehmers erstellt werden (z.B. durch Code-Injektion). Es ist dann die Entscheidung des Teilnehmers, ob er teilnehmen möchte oder nicht. Daher kann das Einwilligungskästchen nicht vorab angekreuzt werden, sondern die Teilnehmer müssen es selbst ankreuzen. Durch diese Maßnahmen ist das System von Adsata vollständig DSGVO-konform.

Auswahl von Studien und Stimuli: Obwohl es sich hierbei eher um ein technisches Hindernis als um eine aktive Entscheidung handelt, ist das System von Adsata nicht in der Lage, Veränderungen der Pupillengröße der Teilnehmer zu erkennen. Dies macht es unmöglich, körperliche oder demografische Merkmale der Teilnehmer allein anhand ihrer Pupillendaten vorherzusagen.

4. Der Weg in die Zukunft

Mit dem Beginn des technologischen Fortschritts ist es klar, dass Webcam-Eyetracking-Systeme eine vielversprechende Alternative zu Hardware für das Eyetracking im Labor darstellen. Obwohl Webcam-Eyetracking-Systeme technologische Einschränkungen in Bezug auf die Datenqualität aufweisen, werden solche Systeme durch Fortschritte bei browserbasierten Technologien (z. B. Tensorflow.js und WebAssembly) weiter verbessert. Diese Technologien bieten zuverlässige browserbasierte Berechnungswerkzeuge zur Verarbeitung großer Datenmengen und gewährleisten gleichzeitig, dass sich die Daten der Teilnehmer in der sichersten Umgebung befinden: ihren eigenen Endgeräten.

Es ist offensichtlich, dass die Technologien für die Augenerfassung per Webcam eine Reihe von ethischen Herausforderungen für die Entwickler des Tools sowie die Nutzer mit sich bringen. Viele dieser ethischen Herausforderungen können mit neueren Technologien überwunden werden, doch einige dieser Herausforderungen hängen davon ab, wie Fachleute solche Instrumente einsetzen. In gewisser Weise kommt es darauf an, wer ‚hinter der Linse' sitzt, wer die Blickbewegungen verfolgt und was sie untersuchen. Da der Mensch den virtuellen Raum immer weiter entwickelt, wird die Frage immer wichtiger, wie wir ethisch korrekt Daten über die menschliche Interaktion sammeln und nutzen können, um visuelle Systeme zu verbessern.

Die erschwinglichen Preise und die Skalierbarkeit von Webcam-Eyetracking-Geräten in Verbindung mit der Ausgereiftheit der Analysemethoden haben Blickdaten zu einer Standardinformationsquelle bei der Untersuchung der Mensch-Computer-Interaktion, des Nutzerverhaltens oder der Kognition gemacht. Eine umfassende Debatte zwischen allen Beteiligten über den Umgang mit Webcam-Eyetracking steht noch aus und wir hoffen, dass dieses Whitepaper dazu beitragen wird eine solche Diskussion zu eröffnen.

Referenzen

[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.