Zu Risiken und Anonymisierungen von Verhaltensbiometrie

Simon Hanisch, Julian Todt, Melanie Volkamer und Thorsten Strufe

Zusammenfassung

Die bestehenden Social-Media-Plattformen erweitern sukzessive die Art, Qualität und Quantität der Daten, die sie über ihre Nutzer:innen erheben. Zu bereits früher aufgezeichneten Daten kommen diverse neue Arten hinzu: Hierzu gehören Körperbewegungen, wie die Handgesten, mit denen die Geräte gesteuert werden, die Augenbewegungen, die von vielen Geräten erfasst werden, aber auch Faktoren wie die menschliche Stimme, oder Herzschläge und Gehirnaktivitäten.

Neben der simplen Identifizierung von Individuen erlauben diese verhaltensbiometrische Merkmale viele Rückschlüsse über Eigenschaften aufgenommener Personen, wie Alter, Geschlecht, Gesundheitszustand, aber auch die Persönlichkeit. Für die Nutzer:innen ist dabei nur noch sehr schwer zu erkennen, welche Rückschlüsse über persönliche Informationen möglich sind.

Als Gegenmaßnahme gegen diese Privatsphäreeinschnitte haben Nutzer:innen oftmals nur die Wahl, ob eine Anwendung auf einen bestimmten Sensor vollständig zugreifen darf, oder gar nicht; wobei Letzteres oftmals damit verbunden ist, dass die Anwendung nicht mehr wie gewünscht, oder gar nicht mehr funktioniert.

Um dieser Diskrepanz zwischen Datenschutz und immer weitreichenderer Datensammlung zu begegnen, bedarf es zunächst Untersuchungen über die in solchen biometrischen Daten enthaltenen Informationen. Zusätzlich werden neuartige Privatsphäre-Einstellungen nötig, in welchen die Nutzer:innen nicht nur wählen können, ob Daten geteilt werden (z.B. von bestimmten Sensoren), sondern auch ob private Eigenschaften durch Anonymisierungstechniken vor dem Teilen entfernt werden sollen.

1. Einleitung

Die Qualität und Quantität, mit welcher unser alltägliches Leben erfasst wird, hat sich bisher stetig erhöht. Von großen, dedizierten, digitalen Ka-

meras, die nicht mehr als 800x600 Pixel aufnehmen können, zu Megapixel-Kameras in Smartphones ist dieser Trend bis heute ungebrochen. Mit Augmented Reality (AR) and Virtual Reality (VR) steht der nächste Schritt in dieser Entwicklung an.

Die Vision von Technologiekonzernen wie Meta ist es, mit AR/VR ein Metaverse zu schaffen, eine digitale Welt, in der wir arbeiten, interagieren und leben werden. Für das Eintreten in diese digitale Welt ist es notwendig, ihre Nutzer:innen genau zu erfassen, um einen digitalen Zwilling zu erschaffen. Dazu werden die Nutzer:innen dauerhaft von einem AR/VR-Gerät aufgenommen, was die Quantität der erhobenen Daten erhöht. Durch den Einsatz neuer Sensorik wie Tiefenkameras, Inertial-Measurement-Units (IMU) und Lighthouse-Tracking werden die Nutzer:innen außerdem in einer noch nie dagewesenen Qualität erfasst.

AR/VR-Geräte zeichnen Körperbewegungen, Handbewegungen, Mimik und Augenbewegungen auf und auch erste medizintechnische Geräte wie Elektroenzephalografie (EEG) und Pulsoxymeter werden bereits integriert. Allen diesen Merkmalen ist gemeinsam, dass sie das Verhalten ihrer Nutzer:innen aufzeichnen. Man spricht von verhaltensbiometrischen Merkmalen.

Verhaltensbiometrische Merkmale erlauben wie physiologisch-biometrische Merkmale (z.B. Fingerabdruck, Gesicht, Iris) die Identifizierung der Nutzer:innen, da auch verhaltensbiometrische Merkmale für jede Person einzigartig sind. Im Gegensatz zu physiologischen Merkmalen lassen verhaltensbiometrische Merkmale jedoch weitere Rückschlüsse auf private Informationen einer Person zu. So lassen sich aus Körperbewegungen das Geschlecht und verschiedene medizinische Besonderheiten ableiten, und Augenbewegungen erlauben weitreichende Rückschlüsse über Charaktereigenschaften[1] und Interessen[2].

Diese Mischung aus dauerhafter Erfassung und Aufzeichnung von verhaltensbiometrischen Merkmalen bedeutet, dass AR/VR Geräte eine große Gefahr für die Privatsphäre ihrer Nutzer:innen darstellen. Zumal die meisten heute vertretenen Anbieter von AR/VR Plattformen ihr Geschäftsmodell auf der Kommerzialisierung der gesammelten Daten basieren und damit die Kommerzialisierung der Nutzer:innen im Mittelpunkt steht. Zum Schutz vor diesen Gefahren bedarf es guter Schutzmaßnahmen für die Nutzer:innen.

1 Kröger u.a., in: Friedewald u.a. (Hrsg.), Privacy and Identity Management, 2020
2 Hess/Polt, in: Science, 1960 (3423)

In dieser Ausarbeitung befassen wir uns daher mit den Risiken und Schutzmaßnahmen für verhaltensbiometrische Daten im Kontext von Mixed Reality (MR). Zum einen möchten wir aufzeigen, welche verhaltensbiometrischen Merkmale es gibt, wofür sie verwendet werden können und welche Risiken für die Privatsphäre damit verbunden sind. Darüber hinaus schlagen wir vor, die bestehenden Privatsphäre-Einstellungen für das Teilen von Daten mit Anwendungen auf mobilen Endgeräten für AR/VR-Plattformen zu erweitern. Abschließend stellen wir kurz zwei allgemeine Ansätze zur Anonymisierung verhaltensbiometrischer Daten vor.

Die Ausarbeitung ist wie folgt gegliedert. Im folgenden Abschnitt 2 beschreiben wir die verwendete Terminologie sowie das Szenario und die betrachteten Angreifer:innen. In Abschnitt 3 diskutieren wir verwandte wissenschaftliche Arbeiten. In Abschnitt 4 geben wir einen Überblick über existierende verhaltensbiometrische Merkmale und in Abschnitt 5 stellen wir unseren Vorschlag für eine datenschutzfreundlichere Datenfreigabe vor. In Abschnitt 6 stellen wir zwei allgemeine Ansätze zur Anonymisierung verhaltensbiometrischer Daten vor. Abschließend ziehen wir in Abschnitt 7 ein Fazit.

2. Terminologie und Szenario

In diesem Abschnitt beschreiben wir die Terminologie und das Szenario, das wir für unsere Ausarbeitung verwenden.

Biometrische Faktoren sind Merkmale die sich durch die Vermessung von Menschen ergeben und spezifisch für bestimmte Personen sind. Unterschieden werden biometrische Faktoren in physiologische und verhaltensbiometrische Faktoren. *Physiologische* biometrische Faktoren beschreibe direkte körperliche Merkmale eines Menschen. Beispiele für solche Faktoren sind das Gesicht, der Fingerabdruck, oder die Iris. Faktoren, die das Verhalten einer Person beschreiben werden als als *verhaltensbiometrische* Faktoren bezeichnet. Beispiele für diese Faktoren sind unser Gang, unsere Sprache oder unsere Augenbewegungen. Neben den biometrischen Faktoren, die eine Person direkt identifizieren können, gibt es auch so genannte *softbiometrische* Faktoren. Sie enthalten wenig Information und erlauben höchstens die Zuordnung von Individuen zu Gruppen. Für sich alleine genommen erlauben sie keine eindeutige Identifizierung und erst durch die Kombination von mehreren dieser Faktoren wird eine Person eindeutig

identifizierbar. Zu den softbiometrischen Faktoren zählen Merkmale wie das Gewicht, die Hautfarbe, das Alter oder das Geschlecht einer Person.

Für die Privatheit von Personen unterscheiden wir zwei Gefahren. Mit *Identifikation* bezeichnen wir den Prozess, der die biometrischen Daten eindeutig einer Person zuordnet. Und mit *Attributinferenz* bezeichnen wir das Ableiten von persönlichen Eigenschaften aus den biometrischen Daten.

Beim Schutz der Privatheit unterscheiden wir zwischen Anonymisierung und Attributsschutz. Mit *Anonymisierung* bezeichnen wir den Prozess, der die Zuordnung zwischen Identität und biometrischen Daten verhindert oder zumindest erschwert. Wichtig ist hier die Unterscheidung zwischen Anonymisierung und Pseudonymisierung. Bei der *Pseudonymisierung* wird die Zuordnung von Identität und biometrischen Daten durch eine Zuordnung mit einem anderen Identifikator ersetzt, während nach der Anonymisierung die biometrischen Daten keiner Identität mehr zugeordnet werden können. Unter *Attributsschutz* verstehen wir eine Methode, die die biometrischen Daten so verändert, dass bestimmte Attribute nicht mehr aus den biometrischen Daten abgeleitet werden können.

Wenn wir eine bestimmte Methode zum Schutz der Privatsphäre betrachten, dann können wir dies nur im Kontext einer konkreten Anwendung tun, für die die biometrischen Daten verwendet werden sollen. Die Anwendung gibt vor welche Informationen in den biometrischen Daten erhalten werden sollen, den Nutzwert der Daten. Ohne einen konkreten Nutzwert könnten die biometrischen Daten auch einfach nicht erhoben werden, um die Privatsphäre eine Person zu schützen. Eine Methode zum Schutz der Privatsphäre hat also immer zwei (oft konkurrierende) Ziele, den Schutz der personenbezogenen Daten und den Erhalt des Nutzwertes der Daten.

Privatsphäre ist etwas Subjektives: Was als privat empfunden wird und in welchem Kontext hängt einzig und allein von den Nutzer:innen ab. Davon hängen die Ziele für den Schutz der Privatsphäre und den Nutzwert ab, so kann es in einem Kontext für die Nutzer:innen das Ziel sein, ihre Identität zu verschleiern, während in einem anderen Kontext die Identifizierung der explizite Nutzen der Daten ist. Ein gutes Beispiel hierfür ist die medizinische Diagnose mit Hilfe biometrischer Daten. Während sie für eine Untersuchung beim Arzt nützlich sind, sollen sie in fast allen anderen Kontexten vermieden werden.

Als Kontext für unsere Ausarbeitung betrachten wird folgendes *Szenario*: Unsere Nutzer:innen wollen verhaltensbiometrische Daten mit einer AR/VR Anwendung teilen, damit diese ihnen selbst und anderen Nut-

zer:innen einen Nutzen bringt. Ein Beispiel für solch eine Anwendung ist ein VR-Chat, in dem sich Nutzer:innen mit ihren Freund:innen für ein Gespräch treffen. Ein weiteres Beispiel kann aber auch eine medizinische App sein, welche die Herzschläge von Nutzer:innen aufzeichnet und zur Analyse an den Hersteller der App übermittelt. Wichtig in diesem Szenario ist, dass die Nutzer:innen ihre biometrischen Daten in die Hände Dritter geben und somit die direkte Kontrolle über ihre Daten verlieren. Um ihre Privatheit in diesem Szenario zu schützen, nutzen die Nutzer:innen eine technische Methode, welche sensible persönliche Informationen aus den biometrischen Daten entfernt oder diese so verschleiert, dass sie nicht verwertet werden können.

Für unsere *Angreifer:innen* nehmen wir an, dass diese in den Besitz der Daten der Nutzer:innen kommen, entweder weil sie selbst die Dienstanbieter sind, oder weil sie anderweitig an die Daten gelangen (z.B. durch ein Datenleck beim Dienstanbieter). Ziel der Angreifer:innen ist es, die Person, zu der die verhaltensbiometrischen Daten gehören, zu identifizieren oder private Eigenschaften von dieser Person zu inferieren. Zur Durchführung ihrer Angriffe verfügen die Angreifer:innen über verhaltensbiometrische Datensätze, mit denen ein biometrisches Erkennungssystem trainiert werden kann, sowie für die Identifizierung über verhaltensbiometrische Referenzmuster der Nutzer:innen, mit denen die Angreifer:innen die Nutzer:innen identifizieren können.

3. Stand der Wissenschaft

Die Identifizierung und das Ableiten privater Informationen von Personen anhand ihrer biometrischen Daten ist ein Thema, das bereits umfassend erforscht wurde. Bekannte biometrische Faktoren sind hier das Gesicht[3], die Stimme[4], der Fingerabdruck[5] oder die Iris[6]. Es wurde auch schon gezeigt,

3 Deng u.a., in: Conference on Computer Vision and Pattern Recognition, 2019
4 Chandolikar u.a., in: International Mobile and Embedded Technology Conference (MECON), 2022
5 Ali u.a., in: *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016*
6 Patil u.a., in: *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016*

dass die Kopf- und Handbewegungen von Nutzer:innen mit VR-Headsets ausreichen, um diese eindeutig zu identifizieren[7].

Für das Teilen von Daten in MR-Anwendungen gibt es bereits erste Arbeiten, die sich mit Aspekten des Problems beschäftigten. Lebeck et al.[8] untersuchten mit strukturierten Interviews in Verbindung mit einer Laborstudie welche Datenschutzbedenken Nutzer:innen von AR-Anwendungen haben. Des Weiteren haben Harborth und Frink[9] in einer Umfrage untersucht, welche Datenfreigaben für mobile AR-Anwendungen Nutzer:innen am gefährlichsten für ihre Privatheit empfinden.

Als Gegenmaßnahme zu diesen Datenschutzproblemen haben sich Raval et al.[10] mit der Verfeinerung der Datenfreigabe von Videodaten beschäftigt. Anstelle des ganzen Videos wird ein Bildausschnitt durch die Nutzer:innen markiert, welcher mit der Anwendung geteilt wird. Petracca et al.[11] schlagen ein Framework vor, welches das unbeabsichtigte Gewähren von Sensorberechtigungen verhindern soll.

Eine weitere vorgeschlagene Verbesserung beim Teilen von Sensordaten besteht darin, die Daten in einer abstrakteren Form mit Anwendungen zu teilen. Jana et al.[12] schlagen vor, anstelle von Videodaten nur Skelett und Posen mit Anwendungen zu teilen, welche die Körperbewegungen der Nutzer:innen benötigen. Für die gemeinsame Nutzung von Videos zur Szenenerkennung schlagen sie vor, diese auf ihre Umrisse zu reduzieren, wodurch sensible Daten wie Dokumenteninhalt und Schrift aus dem Video entfernt werden. Dieses Abstraktionskonzept wurde von Gunzman et al.[13] durch eine Objekterkennung ergänzt, die einzelne Objekte in der Szene erhält und den Rest ausblendet.

PrePose[14] verfolgt ein ähnliches Abstraktionskonzept, allerdings nicht für statische Objekte, sondern für Bewegungen. Über eine Modellierungssprache kann definiert werden, welche Gesten erkannt werden sollen, ent-

7 Pfeuffer u.a., in: Conference on Human Factors in Computing Systems (CHI), 2019
Miller u.a., in: Scientific Reports 10 no. 1, 2020
Liebers u.a., in: Conference on Human Factors in Computing Systems (CHI), 2021
8 Lebeck u.a., in: IEEE Symposium on Security and Privacy (SP), 2018
9 Harboth/Frink u.a., in: Seventeenth Symposium on Usable Privacy and Security, 2021
10 Raval u.a., in: 14th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys), 2016
11 Petracca u.a., in: 26th USENIX Security Symposium, 2017
12 Jana u.a., in: 22nd USENIX Security Symposium, 2013
Jana u.a., in: IEEE Symposium on Security and Privacy, 2013
13 Gunzman u.a., in: IEEE 44th Conference on Local Computer Networks (LCN), 2019
14 Figueiredo u.a., in: IEEE Symposium on Security and Privacy (SP), 2016

sprechend wird der Anwendung mitgeteilt, welche Grundgesten in welcher Reihenfolge ausgeführt werden.

Lehman et al.[15] schlagen vor, nicht die Daten selbst, sondern die darauf arbeitenden maschinellen Lernmodelle (ML-Modelle) zu verändern. In ihrem System müssen Anwendungsanbieter ihre ML-Modelle bei den Plattformanbietern einreichen, die diese auf ihre Funktionsfähigkeit prüfen und zertifizieren. Auf dem Gerät selbst können dann nur zertifizierte ML-Modelle genutzt werden, denen die Nutzer:innen eine Erlaubnis erteilt haben.

Um die Nutzung von MR-Geräten in sensiblen Bereichen einzuschränken haben Roesner et al.[16] vorgeschlagen die MR-Geräte auf physische Schilder reagieren zu lassen. Wenn die Geräte ein Verbotsschild erkennen, schränken sie ihre Aufnahmen automatisch ein.

Durch die Vermischung von realer und virtueller Welt entstehen neuartige Sicherheitsprobleme für die Nutzer:innen. Ruth et al.[17] haben untersucht, wie Berechtigungen für die Manipulation geteilter virtueller Welten realisiert werden können. Ein weiteres Problem für AR ist hingegen, dass virtuelle Objekte die Sicht der Nutzer:innen auf die reale Welt versperren und so z.B. zu Unfällen führen können. Lebeck et al.[18] haben weiter untersucht, wie ein Rechtesystem gestaltet werden kann, das gefährliche Einblendungen in AR verhindert, z.B. das Verdecken von Gefahren in der realen Welt.

Wir sehen in der Literatur, dass das Datenschutzproblem von verhaltensbiometrischen Daten bereits erkannt wurde und auch erste Vorschläge zur Lösung existieren. Was aber bisher fehlt, ist ein Ansatz, wie dieser verbesserte Privatheitschutz den Nutzer:innen einfach und intuitiv zur Verfügung gestellt werden kann und wie allgemeine Anonymisierungen aussehen können.

4. Chance und Risiken von Verhaltensbiometrie

Im Folgenden stellen wir verschiedene verhaltensbiometrische Faktoren vor und gehen auf ihre Nutzen und Gefahren für die Nutzer:innen ein. Wir präsentieren hier keine vollständige Liste verhaltensbiometrischer Faktoren,

15 Lehman u.a., in: ACM Transactions on Privacy and Security 25, no. 4, 2022
16 Roesner u.a., in: ACM SIGSAC Conference on Computer and Communications Security, 2014
17 Ruth u.a., in: 28th USENIX Security Symposium, 2019
18 Lebeck u.a., in: IEEE Symposium on Security and Privacy, 2017

sondern konzentrieren uns auf die wichtigsten Faktoren für Augmented Reality und Virtual Reality.

4.1 Gangerkennung

Der aufrechte Gang ist nicht nur im Vergleich zwischen Mensch und Tier einzigartig, auch zwischen Menschen gibt es große Unterschiede in der Art und Weise, wie sie gehen. Diese Gangmuster dienten in der Vergangenheit beispielsweise zur Erkennung von Freund und Feind[19] und ermöglichen es auch heute noch, vertraute Personen aus großer Entfernung zu identifizieren. Gangmuster können mit verschiedenen Technologien erfasst werden. Optisch durch Videoaufnahmen, durch die Veränderung der Beschleunigung während des Gangzyklus mit Beschleunigungssensoren oder durch die Gewichtsverlagerung beim Überqueren von Druckplatten. Aber auch Technologien wie Radar[20], LiDAR[21], oder WLAN[22] erlauben die Aufzeichnung von Gangmustern. Dabei ist zu beachten, dass die Aufzeichnung von Gangmustern meist nicht im Fokus steht, sondern ein Nebenprodukt anderer Aufzeichnungen wie z.B. Überwachungsvideos ist. Wichtig ist auch, dass Gangdaten relativ einfach ohne Einwilligung der aufgezeichneten Personen erhoben werden können und weniger Abhängig von der Qualität und Blickwinkel der Aufnahme sind als z.B. Gesichter.

Nutzen: Der Hauptnutzen von Gangdaten liegt in der Diagnose von Krankheiten wie Parkinson[23]. Hier werden meist Video- oder 3D-Motion-Capture-Verfahren eingesetzt, um eine genaue Ganganalyse zu ermöglichen. Ein weiterer Nutzen von Gangdaten ist das Zählen von Schritten. Da Gangdaten oft beiläufig bei der Aufzeichnung anderer Daten erfasst werden, ist auch die Erhaltung dieser Aufzeichnungen zu berücksichtigen. Im AR/VR-Kontext ist auch die Animation von digitalen Avataren eine mögliche Anwendung von Gangdaten.

Gefahren: Gangdaten haben ein hohes Identifikationspotenzial, da sie einfach zu erheben sind und bereits die Aufzeichnung eines einzelnen

19 Yovel/O'Toole, in: Trends in Cognitive Sciences 20, no. 5, 2016
20 Wan u.a., in: ACM Computing Surveys 51, no. 5, 2018
21 Gálai u.a., in: International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM), 2015
22 Wang u.a., in: ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2016
23 Abdulhay u.a., in: Future Generation Computer Systems 83, 2018

Schrittes ausreicht, um Personen zu identifizieren[24]. Gangerkennung funktioniert auch mit Videos, die mit geringer Auflösung und aus einem ungünstigen Winkel (z.B. schräg von oben) aufgenommen wurden[25]. Auch lässt sich die Gangerkennung von Nutzer:innen nur schwer verhindern, da es anders als bei der Gesichtserkennung nicht möglich ist, das Gesicht einfach zu verdecken, um sie zu unterbinden. Neben der Identifikation von Personen ist es auch möglich, auf private Attribute wie Geschlecht[26] und Gewicht[27] zu schließen.

4.2 Handbewegungen

Die Fähigkeit, komplexe Handbewegungen auszuführen und damit Werkzeuge zu bedienen, ist ein herausragendes Merkmal des Menschen. In unserem heutigen Alltag benutzen wird unsere Handbewegungen hauptsächlich zur Steuerung von Computern. Damit einher geht die digitale Aufzeichnung unserer Handbewegungen. So sind unsere Bewegungen mit Computermäusen und unsere Tippmuster auf Tastaturen verhaltensbiometrische Faktoren, die ausgewertet werden können. Hinzu kommen Gesten auf mobilen Endgeräten und bei AR/VR-Geräten die Bedienung von Controllern[28] und Freihandgesten.

Nutzen: Handbewegungen spielen heute in der Mensch-Computer-Interaktion als Eingabemodalität eine wichtige Rolle. Aber auch für die nonverbale Kommunikation zwischen Menschen mittels Gebärdensprache oder einfachen Gesten sind Handbewegungen unersetzlich.

Gefahren: Personen können anhand ihrer Handbewegungen identifiziert werden, z. B. durch Tastatureingaben[29] oder Gesten[30]. Auch Krankheiten wie Parkinson[31] können anhand eines verstärkten Zitterns der Hände diagnostiziert werden. Darüber hinaus ist die Semantik von Handbewegungen in bestimmten Kontexten problematisch, z. B. kann aus einer Aufzeichnung der Fingerbewegungen bei der Eingabe eines Passworts auf das Passwort selbst geschlossen werden.

24 Horst u.a., in: Scientific reports 9.1, 2019
25 Wan u.a., in: CM Computing Surveys 51, no. 5, 2018
26 Pollick u.a., in: Human Perception and Performance 31, no. 6, 2005
27 https://www.biomotionlab.ca/html5-bml-walker/
28 Miller u.a., in: Scientific Reports 10, no. 1, 2020
29 Halunen/Vallivaara, in: Secure IT Systems, 2016
30 Clark/Lindqvist, in: IEEE Pervasive Computing 14, no. 1, 2015
31 Jankovic, in: Journal of Neurology, Neurosurgery & Psychiatry 79, no. 4, 2008

4.3 Augenbewegungen

Augenbewegungen bestehen im Wesentlichen aus zwei verschiedenen Bewegungen, den Fixationen, bei denen der Blick auf einen einzigen Punkt gerichtet wird, und den Sakkaden, bei denen die Augen sehr schnell umpositioniert werden. Die Muster, in denen sich diese beiden Grundbewegungen abwechseln, sind von Mensch zu Mensch verschieden und erlauben neben der Personenidentifikation viele weitergehende Rückschlüsse. Augenbewegungen werden mit optischen Verfahren, meist im Infrarotbereich, erfasst. Wichtig dabei ist, dass meist in zwei Richtungen aufgenommen wird, einmal in die Augen selbst, um die Position der Pupillen zu bestimmen, und einmal in die Blickrichtung der aufgenommenen Person. Durch das Zusammenfügen beider Aufnahmen kann festgestellt werden, auf welchen Punkt in einer Szene eine Person ihren Blick gerichtet hat. In der Vergangenheit wurde diese Eyetracking-Technologie vor allem in der Forschung eingesetzt, in den letzten Jahren wird Eyetracking aber auch zunehmend in AR/VR-Headsets integriert.

Nutzen: Augenbewegungen werden in verschiedenen wissenschaftlichen Disziplinen verwendet. In der Medizin liefern Augenbewegungen Informationen zur Diagnose von Krankheiten[32] und zur Untersuchung der visuellen Verarbeitung[33]. In der Psychologie liefern Augenbewegungen wichtige Anhaltspunkte für die Interessen von Proband:innen. Aber auch außerhalb der Wissenschaft werden Augenbewegungen genutzt: In der Werbeindustrie wird die Wirkung von Werbung anhand von Augenbewegungen untersucht. In AR/VR-Headsets werden Augenbewegungen als Eingabemodalität, für das selektive Rendering[34], bei dem der Fokuspunkt der Augen detaillierter gerendert wird als die Umgebung, sowie für die Animation digitaler Avatare[35] genutzt.

Gefahren: Wie bei anderen biometrischen Merkmalen können Personen anhand ihrer Augenbewegungen identifiziert werden[36]. Die Augenbewegungen enthalten ein weites Spektrum an Informationen über den Nut-

32 Harezlak/Kasprowski, in: Computerized Medical Imaging and Graphics, Advances in Biomedical Image Processing, 65, 2018

33 Harezlak/Kasprowski, in: Computerized Medical Imaging and Graphics, Advances in Biomedical Image Processing, 65, 2018

34 Patney u.a., in: ACM Transactions on Graphics 35, no. 6, 2016

35 John u.a., in: IEEE Transactions on Visualization and Computer Graphics 26, no. 5, 2020

36 Katsini u.a., in: Conference on Human Factors in Computing Systems (CHI), 2020

zer:in. So kann z.B. auf das Interesse einer Person[37] geschlossen werden oder auf die psychische Belastung[38]. Darüber hinaus sind Augenbewegungen ein Indikator für eine Vielzahl von psychischen Erkrankungen wie Schizophrenie[39], Autismus[40] oder Psychosen[41]. Auch Rückschlüsse auf die Persönlichkeit sind möglich[42].

4.4 Gehirnaktivitäten

Gehirnaktivitäten werde heutzutage hauptsächlich zu Forschungszwecken oder medizinischen Diagnosen erhoben. Die Gehirnaktivitäten werden dabei als die messbare elektrische Impulse aufgenommen, welche von unseren Neuronen erzeugt werden. Die am meisten verbreitete Methode zur Aufzeichnung ist Elektroenzephalografie (EEG), wobei Elektroden auf der Kopfhaut angebracht werden. Zum heutigen Zeitpunkt ist EEG außerhalb der Forschung und Medizin nicht weit verbreitet, es gibt aber erste kommerzielle AR/VR Geräte, welche begonnen haben EEG zu integrieren[43]. Weitere Methoden[44] zur Aufzeichnung von Gehirnaktivitäten existieren, werden aber außerhalb der Medizin bisher kaum eingesetzt.

Nutzen: In der Medizin wird die Gehirnaktivität für die Diagnose von Krankheiten wie Epilepsie[45] oder Alzheimer[46] verwendet. Auch gibt es Bestrebungen Gehirnaktivitäten zur direkten Mensch-Computer-Interaktion zu nutzen[47]. Eine weitere mögliche Anwendung ist z.B. die Authentifizierung von Personen[48].

Gefahren: In ersten Experimenten konnte gezeigt werden, dass sich Bilder aus EEG-Daten generieren lassen, welche Einblicke in die visuellen Prozesse von Personen zulassen[49]. Auch konnte bereits gezeigt werden,

37 Hess/Polt, in: Science 132, no. 3423, 1960
38 Krejtz u.a., in: PLOS ONE 13, no. 9, 2018
39 Holzman u.a., in: Science 181, no. 4095, 1973
40 Wang u.a., in: Neuron, Volume 88, Issue 3, 2015
41 Ettinger u.a., in: American Journal of Psychiatry 161, 2004
42 Berkovsky u.a., in: Conference on Human Factors in Computing (CHI), 2019
43 https://www.neurospec.com/Products/Details/1077/dsi-vr300
https://mixed-news.com/en/varjo-aero-high-end-vr-headset-gets-brain-interface/
44 Hallinan u.a., in: Surveillance & Society, Vol. 12 No. 1, 2014
45 Subha u.a., in: Journal of Medical Systems 34, 2010
46 Subha u.a., in: Journal of Medical Systems 34, 2010
47 https://neuralink.com/applications/
48 Arias-Cabarcos u.a., in: USENIX Security Symposium, 2021
49 Zeng u.a., in: Biomedical Signal Processing and Control 81, 2023

dass sich aus EEG-Daten Rückschlüsse auf geheime Informationen wie Passwörter ziehen lassen[50]. Darüber hinaus lassen sich aus EEG-Daten auch Informationen über den Konsum von Drogen ableiten[51].

4.5 Menschliche Stimme

Die menschliche Stimme ist vielleicht der bekannteste verhaltensbiometrische Faktor. Durch unterschiedliche Physiologie und erlerntes Verhalten haben Menschen einzigartige Stimmen, die unterschieden werden können. Die Stimme wird im Kehlkopf und im Vokaltrakt des Menschen erzeugt. Aufgenommen wird die Stimme mit Mikrofonen, die heute in den meisten mobilen Endgeräten eingebaut sind. So finden sich Mikrofone auch in den meisten AR/VR-Geräten.

Nutzen: Der Hauptnutzen der menschlichen Stimme liegt in der zwischenmenschlichen Kommunikation. Im AR/VR-Bereich wird Sprache als Eingabemodalität verwendet, z.B. zum Öffnen von Menüs[52].

Gefahren: Neben der Identifikation lassen sich aus aufgezeichneten Stimmen auch die Attribute wie Alter[53], Geschlecht[54], sowie emotionaler Zustand[55] einer Person ableiten. Des Weiteren ist es möglich mit Stimmaufnahmen Personen zu imitieren[56], und so Identitätsdiebstahl zu betreiben.

5. Persönliche Daten besser kontrollieren und schützen

Betrachten wir, wie Daten heute auf Plattformen wie Smartphones und Webbrowsern geteilt werden, so hat sich ein Modell durchgesetzt, bei dem die Nutzer:innen einzelne Sensoren für Anwendungen freigeben. Wir gehen davon aus, dass dieses Modell für MR-Plattformen an seine Grenzen stoßen wird, da es für das Funktionieren von MR-Anwendungen notwendig sein wird, die meisten Sensoren dauerhaft mit der Anwendung zu teilen.

50 Martinovic u.a., in: 21st USENIX Conference on Security Symposium, 2012
51 Matovu/Serwadda, in: IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2016
52 Schwarz, in: IEEE Workshop on Automatic Speech Recognition and Understanding, 2011
53 Jiao u.a., in: Speech Communication 106, 2019
54 Ertam, in: Applied Acoustics 156, 2019
55 Yacoub u.a., in: European Conference on Speech Communication and Technology, *2003*
56 Bendel, in: AI & SOCIETY 34, 2019

Somit werden die Nutzer:innen oftmals keine Entscheidungsmöglichkeit haben.

Wir schlagen daher eine Erweiterung des Modells vor, in der die Nutzer:innen neben der Entscheidung, was geteilt wird, auch eine Entscheidung darüber treffen können, wie diese Daten genutzt werden können. Dafür sehen wir zwei komplementäre Bausteine. Zum einen die rechtliche Zweckbindung nach Einwilligung, wie die Daten genutzt werden dürfen und zum anderen die technische Veränderung der Daten, die bestimmte private Informationen aus den Daten entfernt.

Das Teilen der Daten einzelner Sensoren ist aus drei Gründen problematisch:

1. Zum einen können selbst auf den ersten Blick harmlos erscheinende Daten wie die eines Beschleunigungssensors dazu genutzt werden, Nutzer:innen anhand ihrer verhaltensbiometrischen Faktoren wie Gang und Handbewegungen zu identifizieren. Für Nutzer:innen ist es nur sehr schwer zu verstehen, welche weitreichenden Implikationen die einzelnen Sensordaten mit sich bringen.
2. Für den Einsatz neuer MR-Geräte ist eine permanente gemeinsame Nutzung verschiedenster Sensoren für die Grundfunktionalität der Geräte erforderlich. Bei AR-Geräten muss die Umgebung permanent erfasst werden, damit diese mit Daten angereichert werden kann. Bei VR müssen die Bewegungen des Kopfes und des Controllers permanent erfasst werden, um mit den virtuellen Welten interagieren zu können.
3. Das Teilen von Daten, wie es heute auf mobilen Geräten am weitesten verbreitet ist, erfolgt nach dem Alles-oder-Nichts-Prinzip. Nutzer:innen können nur entscheiden, Daten zu teilen oder dies nicht zu tun. Eine weitere Einflussmöglichkeit, was mit den Daten geschieht, ist nicht vorgesehen.

Aufgrund dieser Probleme sind wir der Meinung, dass das derzeitige Modell des Teilens von Daten bei der Entwicklung künftiger AR/VR-Geräten verbessert werden muss. Daher schlagen wir einen neuen Ansatz für das Problem des Datenaustauschs mit Anwendungen vor. Anstatt nur zu betrachten, was geteilt wird, sollten wir uns darauf konzentrieren, was mit den Daten getan werden kann und was nicht.

Dabei spielen rechtliche und technische Datenschutzmaßnahmen unterschiedliche Rollen. Mit rechtlichen Maßnahmen kann festgelegt werden, zu welchem Zweck die Daten verwendet werden dürfen, indem eine ausdrückliche Einwilligung in die Verarbeitung der Daten zu einem bestimmten

Zweck erteilt wird. Mit technischen Maßnahmen hingegen können Daten verändert werden, um eine bestimmte Datenverarbeitung zu verhindern. Beide Maßnahmen können zusammen genutzt werden, um eine feinere Aufteilung von Daten zu ermöglichen und den Nutzer:innen die Möglichkeit zu geben, gezielte Erlaubnisse und Verbote auszusprechen.

Konkret schlagen wir mit diesen beiden Maßnahmen vor, um eine neue Schnittstelle für den Datenaustausch mit Anwendungen zu realisieren. Anstelle eines einzelnen Sensors wird ein Sensor von einer Anwendung für einen oder mehrere Verarbeitungszwecke angefordert. Ein Beispiel wäre die Anfrage eines Beschleunigungssensors, um Schritte zu zählen, oder die Anfrage einer Kamera, um Social-Media-Filter auf Personen anzuwenden. Neben dieser aktiven Anfrage durch die Anwendung kann der Nutzer über die Schnittstelle auch festlegen, welche Verarbeitungszwecke unterbunden werden sollen. Diese Verbote werden dann durch eine gezielte Verschleierung der Daten umgesetzt. So kann z.B. bei der Weitergabe von Videos die Identifizierung von Personen durch gezielte Anonymisierung von Gesichtern und Körperbewegungen erreicht werden.

Der Vorteil solch einer feineren Datenteilung liegt in der erweiterten Kontrolle, die die Nutzer:innen über ihre (Teil-) Daten ausüben können. Der Nachteil für die Anbieter:innen von Anwendungen liegt darin, dass sie einen Teil ihrer Flexibilität einbüßen. Allerdings ist der Funktionsumfang mobiler Endgeräte heute relativ gut verstanden, so dass Standardfunktionen definiert werden können. Beispiele hierfür sind die Objekterkennung in Bildern oder die Sprachsteuerung von Anwendungen. Ein weiterer Nachteil ist die mögliche Beeinträchtigung der Funktionalität von Anwendungen durch Obfuskation.

Wir erwarten, dass durch die feinere Freigabe von Daten die Anwendungsentwickler genauer überlegen müssen, welche Daten sie für eine konkrete Funktion tatsächlich benötigen, da eine große Menge an Freigabeanfragen den Nutzer:innen negativ auffallen wird. Es entsteht ein potentieller Anreiz zur Datensparsamkeit.

6. Ansätze zur Anonymisierung verhaltensbiometrischer Daten

Für den Schutz von verhaltensbiometrischen Daten gibt es verschiedene Ansätze, die wir in diesem Abschnitt näher beleuchten wollen. Dabei orientieren wir uns an dem Szenario, das wir in Abschnitt 2 vorgestellt haben und betrachten nur Methoden, die anwendbar sind, wenn eine Weitergabe

der verhaltensbiometrischen Daten an Dritte erfolgen soll. Dies schließt Methoden aus, die nur den Schutz der Daten während der Übertragung gewährleisten, wie z.B. Verschlüsselung. Da auch Methoden wie Zugriffskontrolle in einem solchen Szenario nicht anwendbar sind, betrachten wir nur Methoden, die die Daten modifizieren und damit den Schutz der Privatheit realisieren.

Weiterhin ist es wichtig zu beachten, dass die Nutzer:innen mit der Weitergabe die Kontrolle über ihre Daten abgeben, was zur Folge hat, dass jegliche Schutzmaßnahme vorab angewendet werden muss. Es ist nicht möglich, den Schutz der Privatheit zu einem späteren Zeitpunkt zu ändern oder zu verbessern, wenn sich herausstellt, dass er unzureichend ist. Die Angreifer:innen haben somit vollen Zugang zu den geteilten Daten und sind in der Wahl ihrer Methoden, diese zu analysieren, nicht eingeschränkt.

Im Gegensatz zu herkömmlichen personenbezogenen Daten wie Namen, Adressen oder Telefonnummern sind verhaltensbiometrische Daten in ihrer Form wesentlich komplexer. Häufig als Zeitreihen von Sensordaten erfasst, vermischen verhaltensbiometrische Daten personenbezogene und nicht personenbezogene Informationen, und es ist nicht offensichtlich, welcher Anteil oder welche Struktur der Daten personenbezogene Informationen enthält. Die personenbezogenen Informationen sind nicht explizit, was den Schutz der Privatheit erschwert.

Neben diesem Mix aus personenbezogenen und sonstigen Informationen enthalten die Daten eine Reihe von Abhängigkeiten, die den Schutz der Privatheit zusätzlich erschweren und die wir am Beispiel der Gangdaten kurz erläutern wollen. Zum einen gibt es zeitliche Abhängigkeiten, eine einzelne Haltung einer Person in einer Gangsequenz ist immer abhängig von den vorhergehenden Haltungen und hat einen direkten Einfluss auf die nachfolgenden Haltungen. Zum anderen gibt es strukturelle Abhängigkeiten, z.B. hängen die Farben eines Pixels in gewissem Maße auch von den Farben seiner Nachbarn ab. Wird das einzelne Pixel entfernt, kann es durch Interpolation seiner Nachbarn wiederhergestellt werden. Schließlich gibt es physiologische Abhängigkeiten in den Daten. Beispielsweise kann ein Mensch seine Gelenke nicht beliebig weit beugen, oder die Position des Kopfes hängt stark von der Position des Oberkörpers ab.

Diese drei Abhängigkeiten führen dazu, dass verhaltensbiometrische Daten sehr redundant sind und noch viele private Informationen in den Daten enthalten sind, selbst wenn große Teile der Daten entfernt wurden. Deshalb ist die Anonymisierung von verhaltensbiometrischen Daten nicht

trivial. Beispielsweise können einfache Anonymisierungsmethoden wie das Verrauschen einzelner Datenpunkte oder das Entfernen von Datenpunkten scheitern, weil die Redundanz der Daten es ermöglicht, die ursprünglichen Daten wiederherzustellen[57]. Für eine erfolgreiche Anonymisierung der Daten ist es notwendig, die oben genannten Abhängigkeiten in den Daten zu berücksichtigen.

Für die Anonymisierung verhaltensbiometrischer Daten werden im Folgenden zwei allgemeine Ansätze vorgeschlagen, die den in Abschnitt 2 genannten Anforderungen genügen.

6.1 Modellierung

Der erste Ansatz besteht darin, die Abhängigkeiten in den Verhaltensdaten zu modellieren. Die Modellierung ermöglicht es, die Daten als Kombination eines Modells und seiner Parameter auszudrücken. Das Modell kodiert die Abhängigkeiten (z.B. physikalische Bedingungen oder menschliche Physiologie) der Daten und die Modellparameter kodieren die einzelnen Datenpunkte. Da die Datenpunkte in dieser Darstellung unabhängig voneinander sind, können sie leichter anonymisiert werden, z. B. durch die Anwendung von Rauschen. Nach der Anonymisierung können die Datenpunkte in das Modell eingefügt werden, um sie wieder in ihre ursprüngliche Form zu übersetzen. Der Vorteil dieser Methode ist, dass am Ende die Datenpunkte in der gleichen Form wie vor der Anonymisierung vorliegen.

Ein einfaches Beispiel für die Modellierung ist der Bewegungspfad eines VR-Headsets im Raum, wobei die Punkte auf dem Pfad des VR-Headsets voneinander abhängig sind, da sich das VR-Headset kontinuierlich bewegen muss und somit jeder Punkt von seinen Vorgängern abhängt. Anstatt die Daten als einzelne Punkte auf dem Pfad zu betrachten, wird der Pfad des VR-Headsets als Geschwindigkeit und Richtung zu jedem Zeitpunkt ausgedrückt. Die beiden Parameter des Modells, Geschwindigkeit und Fahrtrichtung, sind unabhängig voneinander und können so einfacher anonymisiert werden.

Nun sind die Abhängigkeiten in verhaltensbiometrischen Daten oft sehr komplex und nicht einfach zu modellieren, daher ist unser Ansatz, die für diesen Ansatz benötigten Modelle mit Hilfe von Methoden des maschinellen Lernens zu erstellen. Eine Möglichkeit ist z.B. das Training von varia-

57 Hanisch u.a., in: arXiv, 2022

blen Autoencodern, um eine Repräsentation der Datenpunkte zu erhalten, bei der die einzelnen Datenpunkte unabhängig voneinander sind.

6.2 Transformation

Der zweite Ansatz besteht darin, die personenbezogenen Informationen in den Daten direkt zu entfernen und nur die für die Nutzwert der Daten erforderlichen Informationen zu erhalten. Dies erfordert eine Quantifizierung, wie viele private Informationen und wie viele Informationen für die Nutzwert in den Daten enthalten sind. Wenn beide Werte quantifiziert werden können, kann die Anonymisierung der Daten als Optimierungsproblem ausgedrückt werden, bei dem die enthaltenen privaten Informationen minimiert werden sollen, während die für die Nutzwert erhaltenen Informationen maximiert werden sollen.

Eine Möglichkeit, dieses Optimierungsproblem zu lösen, besteht darin, ein maschinelles Lernmodell (ML-Modell) zu verwenden, das die Daten in eine neue Darstellung transformiert. Beim Training werden der Informationsgehalt für Privatheit und Nutzwert als Verlustfunktionen verwendet, damit das Modell eine Transformation lernt, die das Optimierungsproblem löst. Um zu quantifizieren, wie viel Privat- und Nutzwertinformation noch in den Daten enthalten ist, können biometrische Erkennungssysteme verwendet werden, um eine Schätzung des Informationsgehalts für Privatheit und Nutzwert der Daten zu erhalten.

Ein Beispiel für ein solches System ist eine Gestenerkennung für ein AR-Headset. Ein maschinelles Modell extrahiert aus Videoaufnahmen der Hände die Merkmale, die für die eigentliche Gestenerkennung verwendet werden. Dieses System wird mit einem biometrischen Erkennungssystem zur Bestimmung des Risikos für die Privatheit und einem Gestenerkennungssystem zur Bestimmung des Nutzwerts trainiert.

7. Fazit

Die Erfassung und Verarbeitung von verhaltensbiometrischen Daten rückt mit der Weiterentwicklung des Internets hin zu digitalen Welten auf Basis von AR/VR-Technologien in den Fokus. Verhaltensbiometrische Daten enthalten ein breites Spektrum an sensiblen persönlichen Informationen, die es ermöglichen, Personen zu identifizieren, aber auch Rückschlüsse auf die Eigenschaften von Personen zu ziehen.

Die Art und Weise wie wir heute Daten mit Anwendungen teilen, wird die Privatsphäre der Nutzer:innen bei AR/VR Anwendungen nur unzureichend schützen, weshalb wir neue Möglichkeiten benötigen, um das Teilen von Daten zu kontrollieren.

Eine Möglichkeit besteht darin, die Daten vor der Weitergabe zu anonymisieren. Aufgrund der Komplexität verhaltensbiometrischer Daten ist diese Anonymisierung jedoch nicht trivial. Wichtig für eine effektive Anonymisierung ist die Berücksichtigung aller Abhängigkeiten in den Daten.

Finanzierung

Gefördert durch die Deutsche Forschungsgemeinschaft (DFG) im Rahmen der Exzellenzstrategie des Bundes und der Länder – EXC 2050/1 – Projektnummer 390696704 – als Exzellenzcluster „Centre for Tactile Internet with Human-in-the-Loop“ (CeTI) der Technischen Universität Dresden. Diese Arbeit wurde duch die DFG und dem Forschungsbereich Engineering Secure Systems (46.23.01) der Helmholtz Gemeinschaft (HGF) durch KASTEL Security Research Labs unterstützt.

Literatur

Abdulhay, Enas; Arunkumar, N.; Narasimhan, Kumaravelu; Vellaiappan, Elamaran und Venkatraman, V. (2018): Gait and Tremor Investigation Using Machine Learning Techniques for the Diagnosis of Parkinson Disease. *Future Generation Computer Systems* 83, S. 366–73. doi: 10.1016/j.future.2018.02.009.

Ali, Mouad. M.H.; Mahale, Vivek H.; Yannawar, Pravin und Gaikwad, A. T. (2016):. Overview of Fingerprint Recognition System. In: *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, S. 1334–38. doi: 10.1109/ICEEOT.2016.7754900.

Arias-Cabarcos, Patricia; Habrich, Thilo und Becker, Karen (2021): Inexpensive Brainwave Authentication: New Techniques and Insights on User Acceptance. 30th USENIX Security Symposium (USENIX Security 21), S. 55–72. isbn: 978-1-939133-24-3.

Wang, Shuo; Jiang, Ming; Duchesne, Xavier Morin; Laugeson, Elizabeth A.; Kennedy, Daniel P.; Adolphs, Ralph und Zhao, Qi (2015): Atypical Visual Saliency in Autism Spectrum Disorder Quantified through Model-Based Eye Tracking. In: *Neuron* 88, S. 604-616. doi: 10.1016/j.neuron.2015.09.042.

Bendel, Oliver (2019): The Synthetization of Human Voices. In: *AI & SOCIETY* 34, no. 1, S. 83–89. doi: 10.1007/s00146-017-0748-x.

Berkovsky, Shlomo; Taib, Ronnie; Koprinska, Irena; Wang, Eileen; Zeng, Yucheng; Li, Jingjie und Kleitman, Sabina (2019): Detecting Personality Traits Using Eye-Tracking Data. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, S. 1–12. CHI '19. New York, NY, USA: Association for Computing Machinery. doi: 10.1145/3290605.3300451.

Chandolikar, Neelam; Joshi, Chaitanya; Roy, Prateek; Gawas, Abhijeet and Vishwakarma, Mini (2022): Voice Recognition: A Comprehensive Survey. In: *International Mobile and Embedded Technology Conference (MECON)*, S. 45–51. doi: 10.1109/MECON53876.2022.9751903.

Clark, Gradeigh D. und Lindqvist, Janne (2015): Engineering Gesture-Based Authentication Systems. *IEEE Pervasive Computing* 14, no. 1, S. 18–25. doi: 10.1109/MPRV.2015.6.

Deng, Jiankang; Guo, Jia; Xue, Niannan und Zafeiriou, Stefanos (2019): ArcFace: Additive Angular Margin Loss for Deep Face Recognition. In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR),* S. 4690–99.

Ertam, Fatih (2019): An Effective Gender Recognition Approach Using Voice Data via Deeper LSTM Networks. In: *Applied Acoustics* 156, S. 351–58. doi: 10.1016/j.apacoust.2019.07.033.

Ettinger, Ulrich; Kumari, Veena; Chitnis, Xavier A.; Corr, Philip J.; Crawford, Trevor J.; Fannon, Dominic G.; O'Ceallaigh, Séamus; Sumich, Alex L.; Doku, Victor C. und Sharma, Tonmoy (2004):Volumetric Neural Correlates of Antisaccade Eye Movements in First-Episode Psychosis. In: *American Journal of Psychiatry* 161, no. 10, S. 1918–21. doi: 10.1176/ajp.161.10.1918.

Figueiredo, Lucas Silva; Livshits, Benjamin; Molnar, David und Veanes, Margus (2016): Prepose: Privacy, Security, and Reliability for Gesture-Based Programming. In: *IEEE Symposium on Security and Privacy (SP)*, S. 122–37 doi: 10.1109/SP.2016.16.

Gálai, Bence and Benedek, Csaba (2015): Feature Selection for Lidar-Based Gait Recognition. In: *International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM)*, S. 1–5. doi: 10.1109/IWCIM.2015.7347076.

Guzman, Jaybie Agullo de; Thilakarathna, Kanchana und Seneviratne, Aruna (2019): SafeMR: Privacy-Aware Visual Information Protection for Mobile Mixed Reality. In: *IEEE 44th Conference on Local Computer Networks (LCN)*, S. 254–57. doi: 10.1109/LCN44214.2019.8990850.

Hallinan, Dara; Schütz, Philip; Friedewald, Michael und de Hert, Paul (2013): Neurodata and Neuroprivacy: Data Protection Outdated? In: *Surveillance & Society* 12.1, S. 55-72. doi: 10.24908/ss.v12i1.4500.

Halunen, Kimmo und Vallivaara, Visa (2016): Secure, Usable and Privacy-Friendly User Authentication from Keystroke Dynamics. In: *Secure IT Systems*, S. 256–68. doi: 10.1007/978-3-319-47560-8_16.

Hanisch, Simon; Muschter, Evelyn; Hatzipanayioti, Admantini; Li, Shu-Chen und Strufe, Thorsten (2022): Understanding Person Identification through Gait. arXiv. http://arxiv.org/abs/2203.04179.

Harborth, David und Frik, Alisa (2021): Evaluating and Redefining Smartphone Permissions with Contextualized Justifications for Mobile Augmented Reality Apps. In: *Proceedings of the Seventeenth USENIX Conference on Usable Privacy and Security (SOUPS)*, S. 513-533. doi: 10.5555/3563572.3563599.

Harezlak, Katarzynaund Kasprowski, Pawel (2018): Application of Eye Tracking in Medicine: A Survey, Research Issues and Challenges. In: *Computerized Medical Imaging and Graphics*, Advances in Biomedical Image Processing, S. 176–90. doi: 10.1016/j.compmedimag.2017.04.006.

Hess, Eckhard H. und Polt, James M. (1960): Pupil Size as Related to Interest Value of Visual Stimuli. In: *Science* 132, no. 3423, S. 349–50. doi: 10.1126/science.132.3423.349.

Holzman, Philip S.; Proctor, Leonard R. und Hughes, Dominic W. (1973): Eye-Tracking Patterns in Schizophrenia. In: *Science* 181, no. 4095 S. 179–81. doi: 10.1126/science.181.4095.179.

Horst, Fabian; Lapuschkin, Sebastian; Samek, Wojciech; Müller, Klaus-Robert und Schöllhorn, Wolfgang I. (2019): Explaining the Unique Nature of Individual Gait Patterns with Deep Learning. a*rXiv* doi: 10.1038/s41598-019-38748-8.

Jana, S., A. Narayanan und Shmatikov, V. (2013): A Scanner Darkly: Protecting User Privacy from Perceptual Applications. In: *IEEE Symposium on Security and Privacy*, S. 349–63. doi: 10.1109/SP.2013.31.

Jana, Suman; Molnar, David; Moshchuk, Alexander; Dunn, Alan; Livshits, Benjamin; Wang, Helen J und Ofek, Eyal (2013): Enabling Fine-Grained Permissions for Augmented Reality Applications With Recognizers. In: *Proceedings of the 22nd USENIX conference on Security*, S. 415-430. doi: 10.5555/2534766.2534802.

Jankovic, J (2008): Parkinson's Disease: Clinical Features and Diagnosis. In: *Journal of Neurology, Neurosurgery & Psychiatry* 79, no. 4, S. 368–76. doi: 10.1136/jnnp.2007.131045.

Jiao, Dan; Watson, Vicky; Wong, Sidney Gig-Jan; Gnevsheva, Ksenia und Nixon, Jessie S. (2019): Age Estimation in Foreign-Accented Speech by Non-Native Speakers of English. In: *Speech Communication* 106, S. 118–26. doi: 10.1016/j.specom.2018.12.005.

John, Brendan; Jörg, Sophie; Koppal, Sanjeev und Jain, Eakta (2020): The Security-Utility Trade-off for Iris Authentication and Eye Animation for Social Virtual Avatars. In: *IEEE Transactions on Visualization and Computer Graphics* 26, no. 5 , S. 1880–90. doi: 10.1109/TVCG.2020.2973052.

Katsini, Christina; Abdrabou, Yasmeen; Raptis, George E.; Khamis, Mohamed und Alt, Florian (2020): The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. In: *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, S. 1–21. doi: 10.1145/3313831.3376840.

Krejtz, Krzysztof; Duchowski, Andrew T.; Niedzielska, Anna; Biele, Cezary und Krejtz, Izabela (2018): Eye Tracking Cognitive Load Using Pupil Diameter and Microsaccades with Fixed Gaze. In: *PLOS ONE* 13, no. 9. doi: 10.1371/journal.pone.0203629.

Kröger, Jacob Leon; Lutz, Otto Hans-Martin und Müller, Florian (2019): 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.* doi: 10.1007/978-3-030-42504-3_15.

Lebeck, Kiron; Ruth, Kimberly; Kohno, Tadayoshi und Roesner, Franziska (2017): Securing Augmented Reality Output. In: *IEEE Symposium on Security and Privacy (SP)*, S. 320–37. doi: 10.1109/SP.2017.13.

——— (2018): Towards Security and Privacy for Multi-User Augmented Reality: Foundations with End Users. In: *IEEE Symposium on Security and Privacy (SP)*, S. 392–408. doi:10.1109/SP.2018.00051.

Lehman, Sarah M.; Alrumayh, Abrar S.; Kolhe, Kunal; Ling, Haibin und Tan, Chiu C. (2022): Hidden in Plain Sight: Exploring Privacy Risks of Mobile Augmented Reality Applications. In: *ACM Transactions on Privacy and Security* 25, no. 4, S. 26:1-26:35. doi: 10.1145/3524020.

Liebers, Jonathan; Abdelaziz, Mark; Mecke, Lukas; Saad, Alia; Auda, Jonas; Gruenefeld, Uwe; Alt, Florian und Schneegass, Stefan (2021): Understanding User Identification in Virtual Reality Through Behavioral Biometrics and the Effect of Body Normalization. In: *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, S. 1–11. doi: 10.1145/3411764.3445528.

Martinovic, Ivan; Davies, Doug; Frank, Mario; Perito, Daniele; Ros, Tomas und Song, Dawn (2012): On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. In: *Proceedings of the 21st USENIX Conference on Security Symposium*, 34.

Matovu, Richard und Serwadda, Abdul (2016): Your Substance Abuse Disorder Is an Open Secret! Gleaning Sensitive Personal Information from Templates in an EEG-Based Authentication System. In: *IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, S. 1–7. doi: 10.1109/btas.2016.7791210.

Miller, Mark Roman; Herrera, Fernanda; Jun, Hanseul; Landay, James A. und Bailenson, Jeremy N. (2020): Personal Identifiability of User Tracking Data during Observation of 360-Degree VR Video. In: *Scientific Reports* 10, no. 1. doi: 10.1038/s41598-020-74486-y.

Patil, Sandeep; Gudasalamani, Shreya; und Iyer, Nalini C (2016): A Survey on Iris Recognition System. In: *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, S. 2207–2210. doi: 10.1109/ICEEOT.2016.7755084.

Patney, Anjul; Salvi, Marco; Kim, Joohwan; Kaplanyan, Anton; Wyman, Chris; Benty, Nir; Luebke, David und Lefohn, Aaron (2016): Towards Foveated Rendering for Gaze-Tracked Virtual Reality. *ACM Transactions on Graphics* 35, no. 6, S.179:1-179:12. doi: 10.1145/2980179.2980246.

Petracca, Giuseppe; Reineh, Ahmad-Atamli; Sun, Yuqiong; Grossklags, Jens und Jaeger, Trent (2017). AWare: Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings. In: *26th USENIX Security Symposium*, S. 379–396.

Pfeuffer, Ken; Geiger, Matthias J.; Prange, Sarah; Mecke, Lukas; Buschek, Daniel; und Alt, Florian (2019): Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In: *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, S. 1–12. doi: 10.1145/3290605.3300340.

Pollick, Frank E.; Kay, Jim W.; Heim, Katrin und Stringer, Rebecca (2005): Gender Recognition from Point-Light Walkers. In: *Journal of Experimental Psychology: Human Perception and Performance* 31, no. 6, S. 1247–65. doi: 10.1037/0096-1523.31.6.1247.

Raval, Nisarg; Srivastava, Animesh; Razeen, Ali; Lebeck, Kiron; Machanavajjhala, Ashwin und Cox., Lanodn P. (2016): What You Mark Is What Apps See. In: *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*, S. 249–61. doi: 10.1145/2906388.2906405.

Roesner, Franzisk; Molnar, David; Moshchuk, Alexander; Kohno, Tadayoshi und Wang, Helen J. (2014): World-Driven Access Control for Continuous Sensing. In: *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, S. 1169–81. doi: 10.1145/2660267.2660319.

Ruth, Kimberly; Kohno, Tadayoshi und Roesner, Franziska (2019): Secure Multi-User Content Sharing for Augmented Reality Applications. In: *28th USENIX Security Symposium*, S. 141–158. isbn: 978-1-939133-06-9.

Schwarz, Petr (2011): The Kaldi Speech Recognition Toolkit. In: *IEEE Workshop on Automatic Speech Recognition and Understanding*.

Subha, D. Puthankattil; Joseph, Paul K.; Acharya U, Rajendra und Lim, Choo Min (2010): EEG Signal Analysis: A Survey. In: *Journal of Medical Systems* 34, no. 2, S.195–212. doi: 10.1007/s10916-008-9231-z.

Wan, Changsheng; Wang, Li und Phoha, Vir V. (2018): A Survey on Gait Recognition. *ACM Computing Surveys* 51, no. 5, S. 1–35. doi: 10.1145/3230633.

Wang, Wei, Liu, Alex X. und Shahzad, Muhammad (2016): Gait Recognition Using Wifi Signals. In: *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*, S. 363–73. doi: 10.1145/2971648.2971670.

Yacoub, Sherif; Simske, Steve; Lin, Xiaofan und Burns, John. Recognition of Emotions in Interactive Voice Response Systems. In: *8th European Conference on Speech Communication and Technology (Eurospeech)*, S. 729–32. doi: 10.21437/Eurospeech.2003-307.

Yovel, Galit und O'Toole, Alice J. (2016): Recognizing People in Motion. In: *Trends in Cognitive Sciences* 20, no. 5, S. 383–95. doi: 10.1016/j.tics.2016.02.005.

Zeng, Hong; Xia, Nianzhang; Tao, Ming; Pan, Deng; Zheng, Haohao; Wang, Chu; Xu, Feifan; Zakaria, Wael und Dai, Guojun (2023): DCAE: A Dual Conditional Autoencoder Framework for the Reconstruction from EEG into Image. *Biomedical Signal Processing and Control* 81. doi: 10.1016/j.bspc.2022.104440.