Privacy-Protecting Techniques for Behavioral Data: A Survey

SIMON HANISCH*, Technical University Dresden, Germany
PATRICIA ARIAS-CABARCOS†, Karlsruhe Institute of Technology, Germany
JAVIER PARRA-ARNAU‡, Karlsruhe Institute of Technology, Germany
THORSTEN STRUFE, Karlsruhe Institute of Technology, Germany

Our behavior —the way we talk, walk, or think— is unique and can be used as a biometric trait. It also correlates with sensitive attributes like emotions. Hence, techniques to protect individuals' privacy against unwanted inferences are required. To consolidate knowledge in this area, we systematically reviewed applicable anonymization techniques. We taxonomize and compare existing solutions regarding privacy goals, conceptual operation, advantages, and limitations. Our analysis shows that some behavioral traits (e.g., voice) have received much attention, while others (e.g., eye-gaze, brainwaves) are mostly neglected. We also find that the evaluation methodology of behavioral anonymization techniques can be further improved.

CCS Concepts: • **Security and privacy → Pseudonymity, anonymity and untraceability**.

Additional Key Words and Phrases: privacy, behavioral data, de-identification

ACM Reference Format:
Simon Hanisch, Patricia Arias-Cabarcos, Javier Parra-Arnau, and Thorsten Strufe. 2021. Privacy-Protecting Techniques for Behavioral Data: A Survey. *ACM Comput. Surv.* 00, 0, Article 00 (2021), 43 pages. https://doi.org/10.XXXX/XXXXXXX.XXXXXXX

1 INTRODUCTION

The ongoing digital transformation is leading to an increasingly comprehensive data collection on citizens. Ever improving peripherals, like augmented reality (AR)/ virtual reality (VR) goggles, motion capturing suits and gloves, force-feedback input devices, sensor-rich cell phones, smart watches, and other wearables drastically increase the coverage and resolution at which biometrics and behavioral data of individuals become available for processing at the same time.

*Funded by the German Research Foundation (DFG, Deutsche Forschungsgemeinschaft) as part of Germany's Excellence Strategy – EXC 2050/1 – Project ID 390696704 – Cluster of Excellence "Centre for Tactile Internet with Human-in-the-Loop" (CeTI) of Technische Universität Dresden
†Funded by the Helmholtz Association (HGF) through the Competence Center for Applied Security Technology (KASTEL), topic "46.23 Engineering Secure Systems"
‡Recipient of an Alexander von Humboldt postdoctoral fellow. The project that gave rise to these results received the support of a fellowship from "la Caixa" Foundation (ID 100010434) and from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 847648. The fellowship code is LCF/BQ/PR20/11770009

Authors' addresses: Simon Hanisch, Technical University Dresden, Helmholzstraße 10, Dresden, 01069, Germany, simon.hanisch@tu-dresden.de; Patricia Arias-Cabarcos, Karlsruhe Institute of Technology, Am Fasanengarten 5, Karlsruhe, 76131, Germany, patricia.cabarcos@kit.edu; Javier Parra-Arnau, Karlsruhe Institute of Technology, Am Fasanengarten 5, Karlsruhe, 76131, Germany, javier.parra-arnau@kit.edu; Thorsten Strufe, Karlsruhe Institute of Technology, Am Fasanengarten 5, Karlsruhe, 76131, Germany, thorsten.strufe@kit.edu.

A large amount of such data is shared knowingly, when users post their latest achievements, photos, or opinions on products and current affairs. A much larger amount is collected unnoticed, when individuals browse Web pages, use location services and similar apps, or simply enter smart spaces that are enriched with anything from voice assistants to CCTV cameras.

The corresponding behavioral data is highly descriptive of the captured individual and it reveals a multitude of attributes. They contain strong indicators for routines, habits, and also medical conditions and 'ticks'. Known correlations between physiological features and medical conditions include the detection of depression or consumption of anti-depressants in facial pictures, detection of organ insufficiencies due to the coloration of eyes (hepatitis), or skin (alcohol abuse [43], general fitness [154], and others). A large number of studies have also reported correlations between behavioral data and psychological traits as well as characteristics. Behavioral data can also be used to uniquely identify individuals. Prominent examples across the spectrum include identifying personal traits and characteristics from social media feeds [106], identifying users by their mobility patterns [45] and web-browsing behavior [50]. Gait very prominently has been used to identify individuals [200, 211], and it obviously reveals individual attributes like age, gender, and physiological conditions [160, 195]. This also increases capabilities for credit and social scoring, based on aggregated digital dossiers.

Preserving the privacy, and terminally the dignity of individuals who come in the range of sensors and are captured in their behavior requires more sophisticated approaches than removing direct identifiers (IP address, social security number (SSN), blurring a face) or intuitive quasi identifiers (gender, age, ethnicity) in databases. Note, that the behavioral data captured from humans has both temporal dependencies, as it is captured as a time-series, and physiological dependencies, as human bodies must adhere to both their physiological and general physical limitations. Due to the strong dependency between observations and to the underlying models, the efficacy of randomized, perturbative anonymization also must be critically reviewed. Context information and habits being represented as strong signals in the data further complicate effective anonymization.

A growing corpus of studies is addressing this challenge of anonymizing behavioral data. They focus on a variety of different human traits, ranging from the voice, over gait, to less prominent examples like gestures, heartbeat, and others. A systematic review of all these approaches, which bridges the attempts in extracting the shared conceptual and methodological similarities and highlights both differences as well as roads less traveled is missing, to the best of our knowledge.

For this paper, we hence set out to systematize the corresponding literature. We are more interested in privacy than confidentiality: we do not consider approaches in which an entity encrypts its own data to hide it from access by unintended audiences. We are rather interested in approaches that protect from unintended revelation of information contained in data that is collected and shared for a different, explicit purpose [41]. In other words, we are interested in privacy-enhancing technologies (PETs) for scenarios in which behavioral data are collected by or shared with third parties to perform a specific operation. We deem 'confidential computing', processing based on homomorphic cryptography, or similar approaches in which the data owner is the only entity that learns anything from the data, out of scope of our analysis.

For our study, we followed Kitchenham's guidelines [102] to discover and survey the current state of the art, comprising of 78 distinct studies, extracted from a corpus of 237 initially discovered publications. We identify common applications of behavioral data, to extract sensible measures of utility, as well as common privacy threats with corresponding adversary models. We define a taxonomy of anonymization approaches, informed by the related work from the fields of database publication and anonymous communications. We then provide a detailed overview of the

different anonymization approaches, sorted by the trait they aim to protect. We provide insight into the corresponding applications that define utility metrics, and into the privacy threats, privacy goals, applied anonymization concepts, and the evaluation the corresponding scientists performed, together with the data they chose for their studies. Our main findings are that some traits (e.g., voice) received a lot of research interest while others are mostly neglected (e.g., brain activity, eye-gaze). One reason we found for this is the lack of available datasets for these neglect traits. Further, we find that the general evaluation methodology for behavioral biometric anonymization can be improved by taking stronger adversaries into account.

The rest of the article is organized as follows: §2 describes the background on privacy terminology, as well as the related work and our survey approach. §3 introduces behavioral data, applications, and related privacy concerns. We define our taxonomy of concepts in §4, and survey the field, sorting anonymization techniques by the trait the authors addressed and the conceptual approach taken, in §5. We discuss our insights and general lessons learned in §6 and conclude the article with a summary in §7.

2 BACKGROUND

In this section we first review the relevant terminology utilized throughout this work and the existing surveys on anonymization techniques. We then present the methodology we used to perform the systematic literature review.

2.1 Terminology

Our use of the term **privacy enhancement** or **protection** shall refer to the obfuscation of information from internal and external observers, including the information or service provider, regardless of whether this obfuscation consists in data access control, encryption, minimization of the data revealed, or data modification, perturbation, partial or full, in any manner. In the most abstract sense, the behavioral information to be protected may be composed of various elements, including links or relationships among several pieces of information.

Another important type of information to be obfuscated is directly a user's **identity**, by itself or accompanied with behavioral or profile information. The close relation between personal devices (such as smartphones or wearables) and their users makes distinctive features in said devices potentially unique identifiers. In this respect, we adhere to the terminological convention of regarding **anonymity** as a particular case of privacy, when the data to be protected, without being direct identifiers[1], may be linked with external information to reidentify the individual to whom the data refer.

In the field of statistical disclosure control (SDC) [202], the aim is to protect a microdata set, that is, a database whose records contain information at the level of individual respondents, while ensuring that those data are still useful for researchers. In this field, the concepts of **identity and attribute disclosure** refer to the goal of an attacker to ascertain either the identity of an individual in the microdata set or the confidential attribute/s thereof. In this work, our interpretation of the terms anonymity and privacy will be in the sense meant by the aforementioned concepts of identity and attribute disclosure, respectively.

We shall employ the term **utility** to refer to a quantification of the degree of functionality maintained with respect to that intended by a personalized or information service, despite the implementation of privacy mechanisms that may hide or perturb part of the data, along with the degree of quality of service maintained, despite processing, storage,

[1]Direct identifiers allow to unequivocally identify individuals. For example, it would be the case of SSNs or full names. In an data-anonymization process, direct identifiers are always removed in the very first phase.

communication and scalability overheads incurred by such mechanisms. We stress that utility in this context does not refer to user-interface design.

As pointed out above in the introduction, any PETs poses a **trade-off between privacy and functionality**. The optimization of the privacy-functionality (or privacy-utility) trade-off will refer to the design and tuning of PETs in order to maximize privacy for a desired functionality, or vice versa.

2.2 Related Surveys

Most of the surveys on behavioral data focus on analyzing the uniqueness and suitability of behavioral traits to identify people, comparing the accuracy of different approaches and their applicability. In this line of research, we find surveys covering a range of existing behavioral biometrics for user authentication [10, 114, 120, 132], and others focusing on the review of specific traits, such as gait recognition [200], keystrokes [15, 188], eye gaze [98], or brainwave biometrics [74]. However, the treatment of privacy issues is limited to mentioning that there is potential for sensitive inferences or identity leaks but there is no in-depth discussion about privacy countermeasures.

There is an important stream of research on potential privacy attacks to behavioral data focusing on **attribute inferences** [14, 27, 64, 90], or dealing with user de-identification (i.e., trying to identify a person by their behavioral data) [55, 57, 79, 209]. Dantcheva et al. [42] provide an extensive overview of which sensitive attributes, so called soft biometrics (gender, age, ethnicity, weight, etc.), can be inferred from primary biometrics extracted from image and video data. This survey highlights that protecting privacy of inferred attributes is an open research challenge.

While the current literature on behavioral data underscores the need for privacy defences, work on this area is still emerging and scattered but no comprehensive view of the problem, existing solutions, and challenges has been carried out yet. Ribaric et al. [173] review techniques to protect user's visual and multimedia data from attribute inferences and re-identification [173]. Though they include a section on behavioral data protection, it only covers a limited number of traits (voice, gait, and gesture) and anonymization techniques that apply when these data has been captured as video, audio, or images, but no other sensors are considered. Also closely related, Nhat Tran et al. [194] survey biometric template protection techniques, but they do it generally without entering in details of the anonymization needs of behavioral biometrics. In our article, we go beyond the state of the art by systematically reviewing research works on behavioral data anonymization techniques, examining a comprehensive set of traditional and modern types of behavioral traits for which solutions have been proposed, and considering different types of recording sensors and use-cases. We categorize and compare existing techniques, analyze their associated evaluation approaches and results, and present a summary of challenges pointing at research directions that need attention in future work.

2.3 Methodology

We performed a systematic literature review following Kitchenham's guidelines [102] to identify relevant studies on behavioral data privacy techniques, as it is depicted in Figure 1.

Our guiding research question is **"What techniques are applicable to protect behavioral data privacy?"** From this starting point, the goal is to understand how these techniques work, what is the level of protection provided, and what are the limitations and existing open challenges. To answer these questions, we first explored the literature on biometrics [5, 10, 42, 73, 120, 132, 155, 206] to determine what kind of behavioral traits can be used to identify a person. Next, we used this list of traits combined with the keyword **"privacy"** and the semantically similar terms **"anonymization"** and **"de-identification"**, as search strings in the main academic databases for computer science. Based on these search terms, we compiled works with no constraints on publication date, obtaining a set of 237 papers

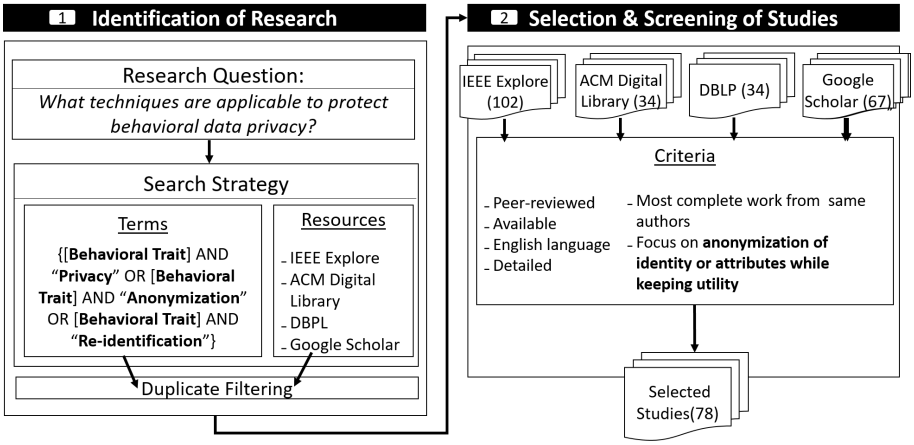

Fig. 1. Summary of the procedure for identifying and selecting relevant studies on behavioral data privacy techniques. We first analyzed the literature on biometrics to determine behavioral traits for person identification. We then used these traits as key terms to search for privacy-related publications, following Kitchenham's guidelines for systematic literature reviews [102]. The complete list of behavioral traits we searched includes: brain activity, eye gaze, facial expression, gait, gesture, handwriting, haptic, heartbeat, kesytrokes, lip, motion, mouse, thermal, touch, and voice.

spanning from 2007 to 2020, after filtering duplicates. During pre-screening, we built a taxonomy of privacy solutions and decided to narrow-down the scope of the survey to anonymization techniques focused on protecting the publication of behavioral data from identity and attribute disclosure attacks. We consider approaches that assume collection, sanitization, and subsequent publishing of data, which must be anonymized but also keep a level of utility to provide behavioral data driven services. Accordingly, the down-selection of primary studies to be analyzed in this survey considered the following criteria. Documents were excluded if:

(1) The publication format was other than peer-reviewed academic journal or conference paper.
(2) The paper could not be retrieved using IEEE Explore, ACM Digital Library, DBLP, or Google Scholar.
(3) The publication language was not English.
(4) Another paper by the same authors superseded the work, in which case the most complete work was considered.
(5) The privacy protection technique was other than identity or attribute anonymization with data utility.
(6) The anonymization approach was described at a high level and not enough details were provided to properly address the guiding research question.

The search and selection protocol yielded a final corpus of 78 peer-reviewed works on behavioral data anonymization, which we clustered according to the behavioral trait being protected: gait, brain activity, heartbeat, eye gaze, voice, and hand motions (handwriting, keystrokes, mouse movements, and hand gestures)[2]. We first describe the different applications of these traits, motivating the need for privacy (Section 3). Then, we define a taxonomy for classifying anonymization techniques (Section 4). We use this taxonomy to review the papers for each behavioral trait (Section 5), analyzing the proposed anonymization technique, its performance, as well as the main advantages and disadvantages. We then examine and discuss the literature in a consolidated way, identifying overall gaps and future challenges to advance research on behavioral data privacy (Section 6).

[2]We found no papers on facial expression, lip, touch, and haptic traits that fulfil our criteria.

3 BEHAVIORAL DATA APPLICATIONS AND PRIVACY CONCERNS

Behavioral data can be leveraged to provide valuable services for both users and companies. In this section, we summarize the application model, the main usages of behavioral data and the related emergent privacy issues, which motivate the need for our survey.

3.1 Behavioral Biometric Data

Behavioral biometric data are a subclass of biometric data which encompasses all human behavior. While in SDC the columns of a microdata set that should be protected are explicit, it is not so easy for behavioral biometrics as it is not apparent which part of the data is privacy sensitive. As behavioral biometric data are captured from a human, it contains a lot of implicit dependencies between individual data points and across traits. For example the motion of a foot is highly depended on the motion of the corresponding leg. Another dependency to consider is the temporal dependency between data points as behavioral biometrics are usually captured as a time-series. These dependencies make the anonymization of behavioral biometric data challenging as an attacker can exploit them to reverse the anonymization.

3.2 Scenario

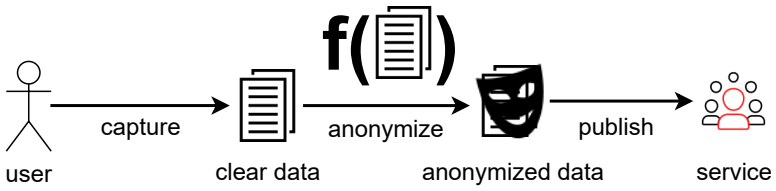

Fig. 2. The data-publishing scenario of the survey.

In this survey, we assume a data-publishing scenario (see Figure 2) in which the data are first transformed in a privacy protective manner and then published or shared with a service or application. This also includes involuntary publication, which for example can occur when the biometric templates of an authentication system are leaked. We assume that the utility of the protected, modified data is preserved to the extent that the received service (e.g., a personalized recommendation) is still meaningful and effective.

3.3 Applications

One of the most important and well researched application area of behavioral data is **biometric authentication** [10, 83, 120, 132]. A person's behavior, such as the way of walking or typing on a keyboard, contain unique inherent patterns that allow for verifying the identity of that person. Given that these patterns can be sensed implicitly while the person interacts with, wears, or carries a device, behavioral biometrics are generally considered more usable than other traditional biometrics like fingerprints [22, 23], and therefore a good alternative or complement to password-based authentication. Academic research has shown the feasibility of numerous behavioral traits for user identification , to name a few: keystroke patterns [188], gait [200], touch [189], mouse movement [218], brain activity [74], or even breathing patterns [33, 34]. And some of them are already developed in commercial solutions, specially in the financial sector to prevent fraud through detecting behavior anomalies [16, 144, 196, 199].

In general the entire of field of **human computer interaction** captures and processes behavioral biometric data, as each input over time also comprises a behavior. Keystroke patterns and mouse movement are our main input modality for computer systems today, however new input modality such as touch, voice, and gestures are on the rise and will likely become more relevant in the coming years.

Another area where behavioral data are useful is **healthcare**. Advances in sensors and machine learning techniques enabled the development of applications for activity recognition, fall detection, and remote health monitoring that facilitate caring of elderly, sick, or disabled people and eases diagnosis [44, 149, 159]. Typical collected data are gait and motion information coming from accelerometers and gyroscopes embedded in user devices, and biosignals like heartbeat or brain activity. This data can be also processed to give health-related feedback to users, for example to guide them through relaxation or to detect and signal cognitive states, such as being stressed, so the user can act on it.

Besides biometric authentication and healthcare, a great deal of behavioral data driven applications are focused on **personalization**. In this category we find adaptive interfaces and services that change their content or appearance according to the predicted user preferences based on their behavior. Furthermore, personalization can be applied in many areas. To give some examples, behavioral data are used to personalize online games adapting to the player profile for a more satisfactory experience (e.g., adjusting the level of difficulty) [222], in recommender systems to suggest online content or advertisements [170], or in education to taylor the learning experience to the student mental state (level of attention, stress, etc.) [93].

3.4 Utility

Depending on each application the behavioral biometric data may be obviously utilized for one purpose or another. For example, in an application for biometric authentication, an evident measure of utility for the provider is its ability to verify the identity of an individual. Likewise, in an application based on human computer-interaction, the provider may require the behavior to still work as reliable input modality for computer systems. In a healthcare application, on the other hand, the service provider may be interested in detecting abnormal behavior patterns, monitoring specific aspects of the behavior such as counting steps or inferring the preferences of a user for personalization, and the utility of the provided service may be assessed as the performance in carrying out those tasks.

3.5 Privacy Concerns

There are also troubling privacy implications derived from the significant amount of personal information implicitly collected in behavioral data driven applications. As we have seen, behavioral data can be used as biometrics because they are rich in individuating information. The counterpart is that any entity that collects behavioral data could use it to identify people even if that is not the main purpose of the service they provide. What aggravates this problem is that people might not be aware that they are being measured, either because of the lack of transparency and adequate consent frameworks, or because the surveillance is meant to be covert. But besides identity, behavioral data carry a wealth of potentially sensitive information that can also be abused. For example, behavioral traits like our voice, eye gaze, gait, or brain responses, are correlated with different diseases [44, 207], mental states and emotions [186, 205], and specific involuntary reactions (such as pupil dilation) can signal our interests [108].

Technically, the general process for inferring identity or other information about an individual from their behavioral data follows four steps, depicted in Figure 3. First, there is a data acquisition step in which the behavioral data are recorded and digitised. Then a feature representation that is suitable for the latter inference is extracted from the raw data. This feature representation is then usually reduced to lower the number of dimensions. In the last step the reduced

feature representation is used to perform the inference of either identity or specific attributes. Thus, machine learning techniques are applied to classify the user data as belonging to an existing user profile or not, or as belonging to a specific attribute class (man, woman). Regression models can also be applied to assign the target individual with a measure (e.g., degree of depression on a continuous 1–5 scale). Based on this general workflow, a service that uses a voice-controlled personal assistant could apply the process to classify the user commanding to open an email application as the owner of the account (authentication). But it could also exploit the voice features to classify the mood of the user and offer them highly targeted advertisements, a practice that often comes with discrimination and threatens user's autonomy. Amazon, for instance, has a patent on technology to extract emotions from user's voice [87].

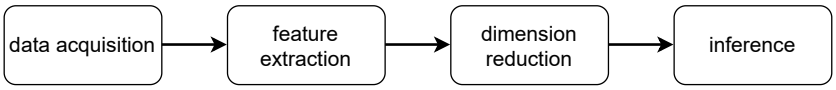

Fig. 3. The general behavioral-based inference process.

While big companies already collect a huge amount of behavioral data, the advent of affordable consumer wearables with numerous sensors (e.g., VR/AR devices with eyetracking, head pose and electroencephalograpy (EEG) sensors) exacerbates the issue. Once the data are collected, even if for a legitimate, user-consented functionality like fraud detection based on behavior anomaly, these data can be exploited to learn private information. Hence, the need for techniques to protect behavioral data is poignant. To establish a map of current research on the topic, we categorize and analyze the existing of protection approaches to prevent from identity and attribute disclosure.

3.6 Attacker Model

Our adversary is a malicious service or application provider that wishes to infer private information about the user. As the service provider the adversary has full access to the behavioral biometric data and can freely select an inference technique. Further, she also might have access to additional prior knowledge about the user such as biometric templates or soft biometrics.

4 A TAXONOMY OF SOLUTIONS FOR BEHAVIORAL DATA PRIVACY

Based on our literature analysis, we identify two main **privacy threats** that apply to behavioral data collected/processed by a third party and can be explained in terms of the related attacker model:

- **Identity Disclosure.** The attacker's goal is to use the behavioral data to identify the user. In this threat model, we assume that the attacker is able to link the target's behavioral data to the target's identity and now wants to identify them in another scenario. For example, linking the user account and data in a work-related application to their account in an entertainment application. This linkage would allow the attacker to learn more about the user activity. An example of this type of attacker, as presented in [182], could be a VR company with devices that record eye-tracking offering several services (e.g., games, adult content, professional training apps). This company would be able to determine if a user is the same person across these applications using their eye-tracking data, even if the user takes care to create accounts with different names or fake personal data. Moreover, it is not uncommon that behavioral data are sold to third parties or released unintentionally through a breach or hack.
- **Attribute Disclosure.** In this threat model, the attacker goal is not to re-identify the user across accounts, but to derive sensitive attributes included within the available behavioral data that the user did not intend to disclose,

such as gender, age, or mental state. The attacker might have had previous access or could have collected a dataset where to train the machine learning model for the targeted inference. For example, based on publicly available electroencephalogram datasets of alcoholic and non-alcoholic persons [97, 143], it could be possible to build a classifier that determines if newly gathered data from a entertainment application using a brain-computer interface (BCI) belong to a user with an alcohol problem.

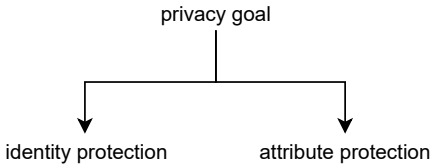

Fig. 4. Taxonomy of anonymization techniques for behavioral data protection according to the privacy goal.

From the privacy threats, we can derive the two **anonymization goals** with which techniques can be categorized, i.e., focused on protecting user **identity** and focused on protecting specific **attributes**, as depicted in Figure 4.

- **Identity Protection**. The process of transforming the behavioral biometric data of person in such a way that that the person can no longer be linked to the data.
- **Attribute Protection**. The process of transforming the behavioral biometric data a person in such a way that specific private attributes of the person can no longer be inferred from the data. Attribute encompasses both long-living attributes such as age or gender and short-living attributes such as mental state or temporary health conditions. An extreme version of attribute protection is template protection. For **template protection** the identification of the person, in the context of an authentication system, should be still possible while all attributes are protected. Further, multiple templates of the same person must not be linkable to each other.

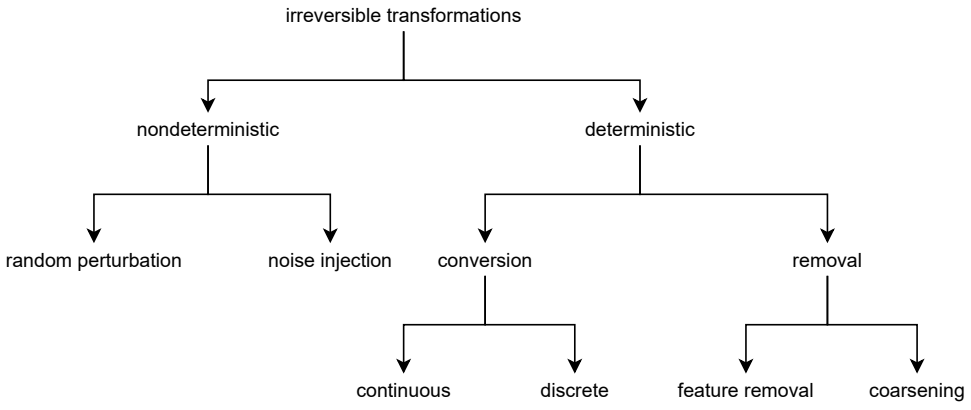

Fig. 5. Taxonomy of anonymization techniques for behavioral data protection according to the type of data transformation applied.

We taxonomize anonymization solutions for behavioral biometric data according to the **type of transformation** applied, as depicted in Figure 5. We include only fundemental concepts, some of the anonymization techniques combine

multiple of them. The basic and shared characteristic of all anonymization methods is that they are irreversible transformations. The first distinction of our taxonomy is if they are deterministic or randomized techniques. **Non-Deterministic methods** rely on randomness in their transformation, which can yield different results for the same input and **deterministic methods** always give the same result. There are several methods under these two approaches, as we detail in the following.

- **Non-Deterministic methods.**
  - **Random perturbations.** A random transformation into a different domain.
  - **Noise injection.** Methods that add random noise to the data points.
- **Deterministic methods.** Are further split into **removal** and **conversion**. The removal method eliminates data points from the data such that the data points do not have an influence on the anonymized result. Conversion methods transform the data points into a new representation, which typically depends on the original domain.
  - **Removal.** Can happen in two forms: **coarsening** and **feature removal**. Coarsening refers to removing parts of each data point or making the data more sparse. Feature removal refers to removing data points belonging to a specific feature altogether.
  - **Conversion.** Can be **discrete** or **continuous**, depending on if the result of the conversion is a discrete or continuous value.

5 ANONYMIZATION TECHNIQUES

We organize the surveyed techniques according to the behavioral biometric trait they seek to protect. The first trait is voice, then we move on to gait, hand motions, eye-gaze, heartbeat, and brain activity. For each of the traits, we analyze their utility, threat space, anonymization techniques, and evaluation methodology.

5.1 Voice

Voice processing and analysis [28] have long been performed and hence a large set of specific terminology exists to describe it. A sound is a change in air pressure, which is often described as airwaves. The sound of the human voice is created by the Larynx and then travels via the vocal tract, which transforms and filters the sound before it leaves the mouth. Due to its approximate tube shape, the vocal tract produces resonances of the sound which are dependent on the length of the vocal tract. Human **speech** is a sequence of sounds that convey meaning. A Phoneme is the smallest unit of sound that distinguishes one word from another and an utterance is a unit of speech between two clear pauses. The frequency spectrum is the range in which the frequency of a sound signal can vary, it is gained from the original signal by using a fast Fourier transform (FFT). An important variant of the spectrum is the log-spectrum which allows a better human interpretation of a signal because the human perception of the magnitude of the signal is roughly approximated by the log transformation. Connecting the peaks in the log-spectrum gives the formant frequencies which correspond to the resonances in the vocal tract and uniquely identify vowels. By using a domain transformation (FFT or cosine) on the log-spectrum we get the cepstrum (see Figure 6). The cepstrum is useful because it allows easy estimation of the fundamental frequency (f0) of the signal. The perceived fundamental frequency by humans is known as pitch. A widely used scale to transform the fundamental frequency to the pitch is the Mel scale. Using the Mel scale the cepstrum can be sampled at frequencies with the same perceived distance using weighted sums. Applying an FFT on those sums gives the Mel-frequency cepstral coefficients (MFCC). The MFCCs are an approximate quantification of the signal spectrum that focuses on the macrostructure of the signal.

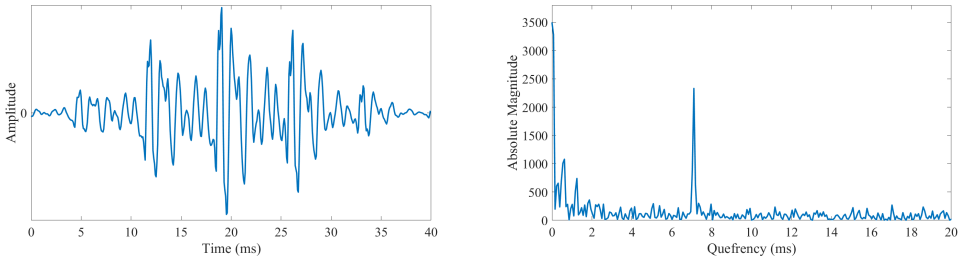

Fig. 6. A windowed speech segment (left) and its corresponding Cepstrum (right), Source: https://wiki.aalto.fi/display/ITSP/Cepstrum+and+MFCC.

The following gives a short overview of the field of speaker recognition which aims to establish the identity of a speaker. Gaussian mixture models [171] (GMM) represent speakers as the distribution of their feature vectors. The feature vectors are extracted from the speech (most often represented as MFCC) of the speaker and then modeled as Gaussian mixture density. A GMM assumes that the data points are generated by a finite number of Gaussian distributions with unknown parameters. Each feature vector is represented as a linear combination of Gaussian densities. A universal background model (UBM) is a GMM that models a wide variety of non-target speakers, representing possible imposters. The means of the UBM are then adjusted to the target speaker by using a maximum aposteriori adaption [172] resulting in a GMM for the target speaker. The benefit of this approach is that the Gaussians used to model the target speaker are the same as in the UBM. For the classification of a speaker, the log-likelihood of the target speaker GMM is compared to that of the UBM to determine if the speaker should be accepted. An alternative to the log-likelihood approach is to get a GMM for each speaker recording through a maximum a posteriori probability (MAP) adaptation of the UBM and then map these GMM to a new feature vector, called Supervector [29]. Supervectors can be classified using traditional methods like support vector machines. A common extension of Supervectors is the total variability (TV) [46] approach. Which maps the Supervectors to a low-dimensional space that models both the speaker and the channel variability. The resulting vector is called i-vector and is the de facto state-of-art in speaker identification. An alternative to i-vectors are x-vectors [179] which are extracted for each utterance via a deep neural network (DNN).

5.1.1 Utility. The main usage of voice recordings is the transmission of information between humans, however, in recent years voice also became an important input modality for computer systems. In both cases, it is important that the content of the speech is intelligible for the intended listeners. But also the mere detection of speech in audio samples can be useful, for example for crowd detection. Further, voices uniquely identify their speaker, making them suitable both for authentication and recognition purposes.

5.1.2 Threat Space. The privacy threats for human voices range from the identification of individuals, over the inference of private attributes, to identity theft via fake recordings. The identification of individuals via their voice has long been apparent to humans. But voices convey more information than just identity, they also allow us to infer attributes such as gender [58], or emotional state [205]. Further, modern speech synthesis methods allow the creation of fake voice recordings for a target speaker, enabling identity theft or the circumvention of speaker authentication systems. Other than the other behavioral biometric traits voice and its resulting speech can also carry a semantic meaning, which can be privacy sensitive.

5.1.3 Privacy Goals. Voice has speech blurring as an additional privacy goal, which aims at destroying the intelligibility of the speech to protect its semantic content from unintended listener.

5.1.4 Anonymization Techniques. We now present the surveyed anoymization techniques that deal with protecting human voices.

Random Perturbation. In [151] Parthasarathi et al. extend their feature removal methods [150] by additionally shuffling the voice blocks. Mtibaa et al. [139] propose a template protection scheme that relies on shuffling the feature vector of a GMM-UBM speaker identification system.

Noise Injection. Tamesue et al. [187] propose a very simple method to make speech unintelligible by simply playing pink noise between 180 and 5630 Hz with various dBs. Hashimoto et al. [78] proposes a system to preserve speech privacy in physical spaces. The core idea is to add white noise to prevent recordings of speakers to be used for identity theft. They found that increasing the Signal-to-noise ratio (SNR) is bad for the intelligibility of the speech and experiment with filtering the white noise in frequency ranges from 0 to 8 kHz to boost the performance of the scheme. They conclude that preventing speaker identity is possible while at the same time keeping the intelligibility of the speech at a high level. Hamm et al. [76] proposes a differential private min-max filter. The mix-max filter minimizes the privacy risk while maximizing utility risk with a given utility and private task. The differential privacy is achieved by adding noises either in front of the filter or after the filter. Ohshio et al. [146] train multiple so-called babble maskers from pre-recorded speakers by segmenting the speech and then averaging the segments. When a speaker should be de-identified the babble masker is selected based on the fundamental frequency and the pitch of the person. Vaidya et al. [197] proposes to add random noise to four features: pitch, tempo, pause, and MFCC.

Feature Removal. In [152] Parthasarathi et al. propose three feature removal methods for privacy-aware speaker change detection. Adaptive filtering assumes that the excitation source is independent of the vocal tract response. They perform short-term linear prediction analysis to estimate an all-pole model [115](representing the vocal tract), a residual (representing the excitation source), and the gain. Then the residual is used to estimate its real cepstrum. Their second method is to remove all subbands except the one from 1.5 kHz to 2.5 kHz and from 3.5 kHz to 4.5 kHz. They represent the two subbands as MFCC coefficients and log-energy from a single filter. Their last method only uses the spectral slope of the speaker represented as cepstral coefficients. In another work [150] also propose similar feature removal methods for speaker diarisation using the real cepstrum and MFCC as features. Their analysis finds that MFCC works better than real cepstrum. Additionally, they add subband frequency information between 2.5 kHz and 3.5 kHz and the spectral slope. The privacy is evaluated by trying to recognize phonemes in the anonymized speech. They use an hidden Markov model (HMM) GMM speaker diarisation method as an evaluation system.

Wyatt et al. [204] propose a feature removal method for speaker segmentation and conversation detection. They segment the audio into segments and save for each the non-initial maximum autocorrelation peak, the total number of autocorrelation peaks, the relative spectral entropy, and the energy of the frame. Zhang et al. [216] uses the same features as proposes by Wyatt et al. except for the energy of the frame and then use an HMM to perform the conversation detection.

In [141] and [142] Nelus et al. propose to use a DNN to extract features from a speaker that allow gender recognition but not speaker identification. Cohen-Hadria et al. [39] use a convolutional neural network called U-net to extract the voices from recordings that consist of both background and voice noise in which the voices should be anonymized. They remove attributes with two methods. The first method simply low-pass filters the voice at 250 Hz. The second

method extracts the MFCC from the voice and then uses the first 5 components to create a new voice. In the end, the blurred speech is recombined with the background noise.

Discrete Conversion. In [153] Pathak et al. present a hashing algorithm to protect voice data for authentication purposes. The supervector of a speaker is gained by performing the MAP adaptation of a universal background model for each utterance of the speaker and concatenating the means of the adapted model. This supervector is the feature vector for the classification. The locality sensitive hashing is then performed with the supervector which transforms it into a low dimensional space, which is referred to as a bucket. This operation is an approximation of the nearest neighbors algorithm. Now the results can be compared to find to authenticate the individual. In order to make the representation more privacy preserving the salted hash of the result is computed. In [162] and [163] Portelo et al. propose a template protection scheme based on secure binary embeddings. The authors use a speaker identification system that uses supervectors and i-vectors to represent the features of a speaker's voice. The feature vectors are then encoded with secure binary embeddings which have the property that if the euclidian distance of the two vectors is below a certain threshold then the hamming distance of the resulting hashes is proportional to the euclidian distance. This allows the comparison of the encoded vectors by using a support-vector machine (SVM) with a hamming distance-based kernel. Billeb et al. [20] propose a template protection scheme that is based on fuzzy commitment. They first extract the frequency spectrum via an FFT and then extract features from the magnitude spectrum. Then the MAP adaptation of a GMM-UBM speaker identification system is applied and additional statistics are extracted. The template is then stored as a combination of error-correcting code and hash algorithm.

Continuous Conversion. **Speaker transformation** is the process of manipulating the voice characteristics of a speaker (not the linguistic features) to make the voice sound like a target speaker. A target speaker can be either a specific natural speaker or a synthetic speaker. For the synthetic speaker either an existing speaker is used or a new one is generated, for example by averaging multiple speakers into one. The general approach of speaker transformation is that the voice characteristics of the source speaker are extracted and then transformed to match the target speaker. In the last step, the new speaker is synthesized.

Jin et al. [92] evaluate four methods for speaker transformation for identity protection. Their base method uses a GMM-mapping based speaker transformation system to transfer speakers to a target synthetic voice called kal-diphone. Further, they test duration transformation in which the length of utterances of the source speaker is scaled to match the ones of the target speaker. Double voice transformation simply repeats the process of mapping the source to the target twice. Lastly, they try an extrapolated transformation in which they use the linear mapping of the source to the target to extrapolate beyond the target. Pobar et al. [158] also use a speaker transformation system based on GMM mapping but combine it with a harmonic stochastic model. The system is trained on a set of speakers to learn the transformation functions. Instead of retraining the system for a new speaker one of the existing transformation functions is applied. This removes the need for a parallel corpus for the speakers that should be protected. The target speaker is a synthetic speaker. In [180] and [95] Justin et al. investigate the intelligibility of transformed speakers. They test with a diphone speech synthesis system and an HMM-based speech synthesis system to transform speakers into a synthetic speaker. They performed a survey with human listeners to evaluate the intelligibility of the protected speakers, measuring the word error rate. Abou-Zleikha et al. [3] do not propose a speaker transformation method themself but explore how to select a target speaker to achieve the lowest identification rate and have good results when the speaker is transformed back to the source speaker. They formulate this as an optimization problem and measure the distance between two speakers with a confusion factor, for which they evaluate entropy and Gini index as metrics. Pribil et al. [164] propose

a speaker de-identification method that relies on modifying several features of the source speaker. In the first step, the prosodic and spectral features are extracted from the source speaker. They then modify the features to make the speaker sound older, younger, more female, and more male by using manually defined transformation functions and feature differences for each class. After the features are modified the de-identified speaker is synthesized.

Bahamanienezhad et al. [13] have developed a speaker transformation method that uses a convolutional encoder/decoder network. They, first extract spectral features and excitation features (f0) from the source speaker. The spectral features are then mapped via the encoder/decoder framework to a target speaker. The resulting speech is fused together either via taking the average or via a gender-based average to create an average speaker. From the excitation features, only the fundamental frequency is transformed via linear transformation, the remaining features stay the same. Both spectral and excitation features are used to synthesize the de-identified speaker. Fang et al. [60] use a similar averaging approach but rely on x-vectors. They extract the x-vector of a speaker and then use a set of random x-vectors of unrelated speakers to calculate a mean x-vector. They also propose to construct an altogether new x-vector that has a similarity scoring of s to the original x-vector. Further, they keep the fundamental frequency of the speaker the same. Kesking et al. [100] do not study de-identification directly but instead try to create an imposter transformation for a target speaker. They use a cycle generative adversarial networks (GAN) voice converter to transform speakers and then evaluate against four speaker identification systems to see if the target speaker is recognized.

Frequency warping is a technique that is similar to speaker transformation, the main difference is that frequency warping focuses on transforming the frequency spectrum of a speaker and usually does not try to transform the source into a specific target speaker. It is mostly used for identity and gender protection. A common goal of frequency warping is vocal tract length normalization in which the resonances that are specific to an individual's vocal tract length should be removed or altered.

Faundez-Zanuy et al. [61] explore two approaches for gender protection: Phase vocoder and vocal tract length normalization. The vocoder approach detects peaks in the voice signal. For each peak, a bin is defined and compared to its two neighbors to define a region of influence. Then the peak and its region of influence are shifted by a peak specific frequency. In the last step artifacts from the shift are removed. The vocal tract length normalization approach defines frames on the signal spectrum and stretches or compresses them using a frequency warping function.

In [1] Valdivielso et al. present a speaker protection approach that transforms the pitch and the frequency axis. Further, the parameters of the transformation are embedded into the signal for later re-identification. Lopez-Otero et al. [118] rely on frequency warping and amplitude scaling for speaker protection in the context of depression detection. They implement both operations as an affine transformation in the cepstral domain and manually define piece-wise linear transformation functions.

Magarinos et al. [119] also relies on frequency and amplitude warping for speaker protection. First, they extract the cepstral voice vectors from the speaker and then convert them into a discrete spectrum. Then dynamic frequency warping (DFW) is applied to map the source spectrum bins to the target spectrum. As multiple source bins can have the same target bin, all source bins that map to the same target bin are averaged. Additionally to the frequency and amplitude warping the fundamental frequency is adjusted regarding its mean and variance. Aloufi et al. [9] try to hide the emotional state of speakers before their speech is sent to a voice-based cloud service. They first extract the fundamental frequency, spectral envelope, and aperiodicity. The features are then transformed via a cycle GAN from emotional speech to neutral speech.

Srivastava et al. [181] evaluate multiple speaker protection methods against an informed attacker. They work with three attacker models: An ignorant attack that is not aware that the voice data is de-identified, a semi-informed attacker

that knows that the data is de-identified, and an informed attacker that knows the de-identification method and its parameters. The first method is a vocal tract length normalization approach. The speaker is represented as a set of centroid spectra. The algorithm then calculates the closest path between the source set and the target set to get the parameters for the warping. The second method uses a neural net encoder/decoder approach to transform the speaker.

Continuous Conversion + Random Perturbation. Canuto et al. [32] proposes a new method for template protection in which the feature vector is shuffled via a randomized sum. For each feature vector, the elements are shuffled based on a secret key. Two random vectors of the same length are derived from the key. These vectors give the position of the attributes that should be summed. The reorganized feature vector is summed up with the vectors resulting when the position vectors are applied to the original feature vector.

Continuous Conversion + Noise Injection. In [103] and [104] Kondo et al. create so-called babble maskers by segmenting speech into ten second segments and then averaging them into babble maskers. Besides speaker-dependent maskers, they also create gender-based babble maskers based on multiple speakers of the same gender. The babble masker is then applied to the recording of the speaker. Qian et al. [166] present a method to sanitize speech before it is sent to the server of a virtual assistant. Their main method is to perform vocal tract length normalization via a compound frequency warping function consisting of a bilinear and a quadratic function to avoid re-identification attacks. The parameters of the warping function are selected randomly. Additionally, they add Laplace noise after the warping function to make the anonymization more robust. For the result, they claim to achieve differential privacy. In [165] the same authors further investigate the security of their scheme. Srivastava et al. [181] also investigate the security of the scheme with stronger attackers.

5.1.5 Evaluations. Qian et al. [167] present a framework to reason about the privacy and utility of voice anonymization techniques. For this, they present the measure of p-leak limit which should give a maximum privacy leakage per speaker for a published dataset. Zhang et al. [215] propose a theoretical framework to quantify the privacy leakage risk and utility loss for speech data publishing. They identify three main data properties to anonymize: dataset description, speech content, and speaker voice. For speaker de-identification they do not describe their own speaker de-identification techniques but give a framework for quantifying the utility privacy loss.

Most of the reviewed works evaluate the quality of the de-identification by comparing the recognition rates of attributes or identities on unmodified and de-identified data. The recognition is done via machine learning models or human listeners. As metrics to measure the recognition rate the papers mostly rely on the equal error rate (EER), false positive rate (FPR), false negative rate (FNR), recall, precision, and F1 score. Abou-Zleikha et al. [3] also use entropy and the Gini index to evaluate the de-identification performance.

Additionally to the de-identification, some works evaluate the loss of utility. One important goal in regards to human listeners is to achieve a natural-sounding de-identified voice. The naturalness is evaluated by human listeners using the mean opinion score. Another important aspect is the intelligibility of the de-identified speech. Intelligibility can be evaluated via human listeners or machine learning models using the word error rate, phoneme error rate, or short-time objective intelligibility.

A common limitation we observed is that in most evaluations use the clear data to train the recognition model and then test it against the anonymized data. This approach implicitly assumes that the attacker is not aware of the anonymization and hence does not try to circumvent it. A work that explicitly assumes an attack on the anonymization is [181]. Here the authors propose attackers with varying degrees of information about the performed anonymization.

5.2 Gait

The human gait is the pattern in which humans move their limbs during locomotion, multiple manners of gait exist such as trotting, walking, or running. Gait can be broken down into individual gait cycle [183] (see Figure 7) which is the shortest repetitive task during the gait. The gait cycle spans from a specific gait event of one foot until the same foot reaches the same gait event. It consists of a stance phase, in which the foot is on the ground, and a swing phase, in which the foot is in the air. The two phases alternate for each foot. Due to its usefulness as a behavioral biometric trait for identifying individuals, gait has long been a research interest of both computer science and psychology. For example, Yovel et al. [211] find that it plays an important part for humans to identify people at a distance, and Pollick et al. [160] show that it is possible for humans to infer the gender of a walker, even when the walker is only shown as a set of points, as so-called point-light-display. The following section deals with the anonymization of gait patterns.

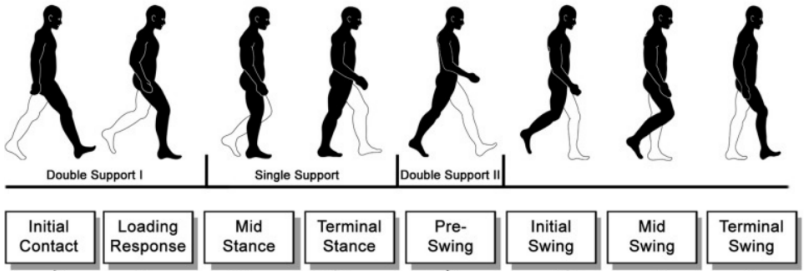

Fig. 7. The phases of the gait cycle, source: [183].

Gait recognition methods have been an active research topic in the past, hence a large set of different methods for various capture methods exists. Wan et al. [200] performed a recent survey on the subject and list recognition methods for cameras, accelerometers, floor sensors, and radars. The main portion of the works focuses on camera based gait recognition which is classified by Wan et al. as either model-based or model-free. Model-based methods use a specific model of the walker, for example, a pendulum model of the legs, to then match the walker to it. Model-free methods, however, do not have an explicit model but rather use the entire capture of the gait to perform the recognition, for example by averaging the silhouette of the walker over time as a gait energy image. Accelerometer-based systems also average the gait into a feature representation either by segmenting the gait into its gait cycles or by using frames with a fixed size.

5.2.1 Utility. The human gait is omnipresent in everyday life and as such often captured as a byproduct of recordings being made. As such it is often not necessary to preserve the utility of the gait, but rather the utility of the recording. One example of this would be video recordings of people walking, the gait pattern itself is not so important but rather that the video looks natural and convincing to its viewers. But there also exist use-cases in which the gait pattern itself should be captured, for example for medical examinations by a physician to find gait abnormalities. Another more casual example would be the recording of the gait pattern to count the steps a person has performed during a day.

5.2.2 Threat space. Due to its omnipresence in everyday life, human gait is easy to capture, especially because most capturing methods are unintrusive and do not require the participation of the victim. Additionally, it has been shown that gait recognition is very robust to video quality and obfuscation making it very much suited for surveillance systems [200]. Besides identifying humans it has also been shown that gait can be used to infer private attributes like

gender [160]. Considering all this the threat to gait biometrics is already large. What's more, with recent developments in richer capturing methods such as LiDAR [65] or cheap motion capture suits, it is to be expected that the threat space for gait will even increase in the coming years.

5.2.3 Anonymization Techniques. In the following, we present the gait anonymization methods found in the literature, sorted by our taxonomy.

Random Perturbation. Hoang et al. [82] propose a fuzzy commitment scheme based on Bose–Chaudhuri–Hocquenghem (BCH) codes for storing accelerometer gait templates. After the feature extraction and binarization of the accelerometer data the reliable bits are extracted. These bits are then XORed with the BCH encoded secret key to gain the secure γ. Additionally to the γ, the hash of the secret key and some helper data are stored. During the authentication phase, the extracted reliable bits are XORed with the secure γ and then decoded with BCH. The result can then be hashed and compared to the hash of the secret key.

Noise Injection. The influence of noise injection on the performance of accelerometer/gyroscope authentication systems was studied by Matovu et al. [129]. For their approach, they generate a time series of noise values drawn from a uniform distribution and then merge the original time series with the generated one. The two traits evaluated are gait and handwriting.

A noise injection approach for gait in videos was developed by Tieu et al. [192]. They use a convolutional neural network (CNN) to mix the gait of a second person (noise gait) into the original gait. In the first step, the silhouette for both the original and noise gait is extracted from a black and white representation of the input videos. The noise gait is selected hereby to have the same size and view angle as the original gait to achieve a more natural result. The silhouettes are then fed into the CNN which uses shared weights networks to abstract them and then merges the abstracted representations via a third network. In a post-processing step, the original gait is replaced with the newly merged gait. The authors further improve their method in [193]. Here the noise gait is generated via a generative adversarial network (GAN) that takes Gaussian noise as input and outputs noise silhouette. Instead of using a CNN they then use a self-growing and pruning GAN (SP-GAN) to fuse the noise and original gait. Further, they propose an approach to colorize the resulting black and white silhouette. In [191] it is proposed to use a deep convolutional GAN to fuse original and noise gait.

Feature Removal. A feature removal approach for privacy-preserving activity recognition via accelerometers is proposed by Jourdan et al. [94]. They extract various temporal and frequency features from the accelerometer data such as mean, correlation, energy, or entropy. Via experiments, they then determine the influence of each feature for activity and identity recognition. They find that the temporal features contribute more to identity recognition and frequency features more to activity recognition, therefore they remove the temporal features.

Continuous Conversion. A continuous conversion approach is blurring, in which persons in videos, including their gait, should be de-identified. As a first step, the silhouettes of the persons in the videos are tracked and segmented to then apply the blur. Agrawal et al. [7] proposed two blurring approaches exponential blur and line integral convolution (LIC). Exponential blur regards the video as a 3D space with the time as the z-axis and then calculates a weighted average of the neighbors of each voxel to blur via an exponential function. LIC works with the bounding box of the walker silhouette and maps it onto a vector field which is then used to calculate the output pixels. To counter reversal attacks against the blur randomization of the blurring functions at each pixel is proposed. Another blurring approach is

proposed by Ivasic-Kos et al. [91]. They apply a gaussian filter to blur the silhouettes of walkers. The filter calculates a weighted average of the color of the neighboring pixels, with the weights decreasing monotonically from the central pixel.

Continuous Conversion + Discrete Conversion. An approach that combines both continuous and discrete conversions for walkers in videos is proposed by Hirose et al. [81]. First, they extract the silhouette and the gait cycle of the walker. The silhouette is then transformed via a deconvolutional neural network encoder into a silhouette code. The code is converted by using a k-same approach in which the k-nearest neighbors of the input code are selected and then a weighted average is computed. The gait cycle is transformed via a continuous, differentiable, and monotonically increasing function. In the last step, the new video is generated by feeding the perturbed silhouette code and gait cycle into the convolutional neural network decoder.

5.2.4 Evaluation. Gait de-identification is evaluated in the literature via gait recognition systems or human observers with the recognition accuracy as the main metric, but there are also usages of the F1 score, equal error rate (EER), or false acceptance rate (FAR). To access the utility loss there is a larger variety of metrics, usually to either quantify the naturalness of the de-identified gait or to perform another kind of recognition, such as activity. One specific evaluation method we observed was [129] in which the authors use the biometric menagerie to observe the de-identification influence on different types of users in biometric authentication systems.

5.3 Hand Motions

Hand motions are the wide variety of movements humans can perform using their hands. As they are such a universal part of human interaction with their environment there exist multiple approaches for using hand motions a behavioral biometric factors: handwriting, keystrokes, mouse movements, and hand gestures. They differ by how the hand motions are recorded and which task the person performs. Handwriting is a hand motion in which the person performing it uses a pen to write text. Due to the uniqueness of people's handwriting, it has long been established that humans can be identified by it. Signatures are the written name of a person which are intended for identification purposes, for example on legal documents. Handwriting can be captured offline in which the produced text is captured via a picture or online in which the movement of the pen is captured during the writing process. For this survey, we only consider the uniqueness of one writing style and not the linguistic style (Stylometry) of the written text. In modern life, handwriting has been largely replaced by typing on a keyboard. Besides writing texts, keyboards are also used as a general input modality for computer systems. The keystrokes and the timings a human produces while using a keyboard are also a biometric factor. Another input modality that captures hand motions are mouse movements. Hand gestures are the wide range of hand motions humans perform to communicate nonverbally. While a normal part of human communication, hand gestures only recently became important as an input modality for computer systems with the rise of swipe gestures on smartphones. This trend is continuing with freehand gestures for wearables such as smartwatches or augmented reality headsets.

Hand motion recognition encompasses multiple recognition techniques for different capture modalities, here we give an overview of handwriting, mouse movements, keystrokes, and gestures. For handwriting bases hand motion recognition the input handwriting sequence is often adjusted for its baseline, scaled to a normal writing style, and segmented to meet the demands of the classifier [156]. Handwriting is further dependent if it was captured while the person was writing (online handwriting), for example with a digital pen, or only handwriting itself is capture after the person has finished (offline handwriting). The recognition for mouse movements relies on the trajectory, speed, single,

and double clicks performed with a mouse as features. Keystroke-based hand motion recognition is based primarily on the timing differences between button up, down, and hold events. Besides individual events, the differences between two successive events or even three successive events are also used as features [221]. Hand motion recognition via gestures can be split into 2D gestures which are performed on a flat surface (e.g. on a smartphone) and 3D gestures which are performed in mid-air. [177] uses the trajectories of each finger and first resample them using a cubic spline interpolation to get a lower sampling rate, removing unwanted jitter. They then use a mutual information metric to classify the gesture. [175] In the first step they label each finger. Then the distance between every two fingers and each finger position and its following position is calculated. To find the distance between two gestures dynamic time warping is employed with various distance metrics. [190] The 3D gesture recognition works similar to the 2D one as first the fingertips of each finger are found and then after scaling and smoothing multiple features based on the fingertips are selected. The classification is again performed with dynamic time warping.

5.3.1 Utility. The utility range for hand motions is a large and diverse field. For handwriting the resulting text must be readable either by humans or computers, the particular handwriting style is usually not important. This is different for signatures, as their main purpose is to facilitate the identification and verification of the signers identity, hence their particular style is important, while the readability of the name is less important. Since the other hand motions mostly serve as input modalities for computer systems their utility as input modality must be kept precise and timely to keep their utility as an input modality. For hand gestures, there is additionally its utility for non-verbal communication.

5.3.2 Threat Space. Handwriting used to be essential to human communication but with the rise of computers, it has become less important and was mostly replaced by digital communication. Due to its decline as a communication medium, it has become difficult to get handwriting samples of a particular person. Since the sensitive nature of signatures as a biometric factor is commonly known humans are usually cautious at leaving their signature, however, due to them widely being used in everyday life there still at risk of being collected by an adversary. Most hand motion capturing today happens implicitly when humans use their hands to control computer systems. Each time we use a mouse or keyboard our hand motion is recorded and as such at risk. Most applications or websites could be used to capture both mouse movements and keystrokes. But even without direct access to the keyboard attackers could collect these biometrics via side-channels such as network latency. Hand gestures are a rather new input modality for computer systems and only became widely popular with the rise of smartphones. Due to their exposed nature and the fact that we often perform gestures in public hand gestures are relatively easy to capture by an adversary, for example by using a camera. It is to be expected that with the rise of mixed reality and its applications hand gestures gain more importance as an input modality and therefore will be at a higher risk.

5.3.3 Anonymization Techniques. In the following, we present the suitable methods for hand motion anonymization, with the exception of mouse movements as we did not find any suitable papers for it.

Random Perturbation. Maiorana et al. [122] propose a template protection method for online handwriting which splits a handwriting sequence into segments and then randomly mixes the segments before convoluting them. The same shuffling approach is taken by Maiti et al. [123] to prevent keystroke inference attacks via wrist-worn accelerometers, however, they do not convolute the segments. Another study investigating the permutation of keystrokes is performed by Vassallo et al. [198]. Goubaru et al. [72] propose a template protection scheme for online handwriting templates. They extract the pattern ID for a user by using a common template. The pattern ID is then XORed with a secret that

was encoded by an error-correcting code. The result is stored as the template. For the verification, the pattern ID is again extracted and then XORed with the template.

Noise Injection. To prevent the identification in browsers via keystroke timings Monaco et al. [135] investigate two noise injection strategies: delay mixing and interval mixing. Delay mixing adds random noise to the timing of a keystroke and interval mixing which draws a new arrival time for each keystroke, depending on a randomly drawn interval. A similar approach to delay mixing is also investigated by Migdal et al. [133] which also add delays to keystroke timings.

Coarsening. Vassallo et al. [198] explore suppression of keystrokes to preserve the content of the typed text in a continuous authentication scenario. Maiti et al. [123] propose two coarsening methods to prevent keystroke inference attacks via wrist-worn accelerometers. In their first approach, they simply detect if a user is typing via several features and then block the access to the accelerometer data to prevent attacks. Their second method reduces the sampling rate of the accelerometer.

Discrete Conversion. An online handwriting template protection scheme is proposed by Sae-Bae et al. [174] which decomposes signatures into histograms on which the authentication is performed. They use one-dimensional histograms to capture the distribution of single features and two-dimensional histograms to capture the dependence between two features. Migdal et al. [134] propose a template protection scheme for multiple modalities, including keystrokes. Their scheme combines multiple pieces of information, such as ip addresses, with the keystroke information and then computes a biohash on it.

Leinonen et al. [112] investigate the anonymization of keystroke timing data using two rounding approaches which effectively sort the timings into buckets. Vassallo et al. [198] explore substitution of keys with a random nearby key to preserve the content of the typed text in a continuous authentication scenario. Figueiredo et al. [63] have developed a modeling language that can be used to design new gestures for applications. Each gesture is validated to check if the gesture can harm the person performing it and if an existing gesture is overwritten by it. The gestures can then be recognized on the recording hardware, eliminating the need to give the application access to the clear data.

Continuous Conversion. Maiorana et al. [122] propose two continuous conversions for online handwriting templates: A baseline conversion which first splits a handwriting sequence into multiple segments based on a secret key and then convolutes the segments. And a shifting transformation that applies a shift to the initial sequence. The template matching is performed on the protected template.

5.3.4 Evaluation. Hand motion anonymization is mostly evaluated in the context of authentication and as such the false positive rate (FPR), false negative rate (FNR), and equal error rate (EER) are important metrics for evaluating the performance. But there is also the usage of recognition approaches for the evaluation for example by [135] which uses the accuracy of identity, age, gender, and handedness inference. A unique evaluation approach we found was used by Goubaru et al. [72] who used the randomness of the template bits via occurrences and autocorrelation to evaluate their approach.

5.4 Eye-Gaze

Eye gaze involves two type of movements: **fixations** and **saccades**. Our eyes alternate between them during visual tasks, such as reading (see Figure 8). Fixations refer to maintained visual focus on a single stimulus, while saccades are

rapid eye movements between fixations to reorient our gaze. Besides, even during fixations, our eyes are not completely still, but constantly producing involuntary micro movements (hundreds per second) known as microsaccades [4].

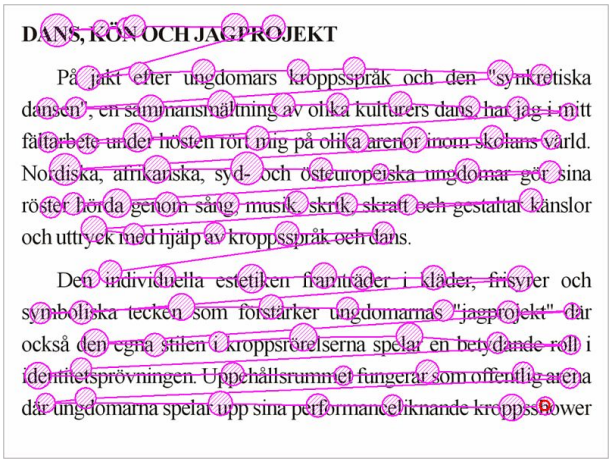

Fig. 8. Fixation and saccades while reading, from a study of speed reading made by Humanistlaboratoriet, Lund University, in 2005. Source:http://en.wikipedia.org/wiki/File:Rea.

Eye-tracking technologies are becoming increasingly available in the consumer and research market. The most common type of tracking technology works by illuminating the eye with an array of non-visible light sources that generate a corneal reflection. These reflections are sensed and analyzed to extract eye rotation from changes in reflections. There is a wide range of hardware configurations for eye-tracking, including embedded cameras in computers, smartphones and virtual reality headsets, dedicated external hardware, or mobile eye-wear. These sensors allow to extract measurements not only regarding movement data related to fixations and saccades (speed, gaze angle, attention spots, scan path), but also additional features, such as pupil size variations and blink behavior. Combinations of these features provide valuable information to implement eye-gaze driven applications.

5.4.1 Utility. Eye movements have been studied, analyzed and used for more than a century in different research domains. In the medical field, gaze provides useful information about our cognitive and visual processing [12, 77], which can be used for diagnosing different diseases. In computer science, eye gaze is used as a form of human computer interaction to improve accessibility, user experience, and to adapt system behavior [40, 124, 161]. More recently, security and privacy researchers have focused on analyzing stable unique features of eye movement to build biometric authentication systems [98]. Behavioral eye biometrics have been subject of intense investigation in the last decade, showing EERs as low as 1.8% [56]. Across all these different domains, the utility to be preserved would depend on the underlying application, e.g., accuracy in predicting the next eye movement, in diagnosing a mental disease, in detecting the focus of user attention, or in recognizing a user.

5.4.2 Threat Space. Eye movement data is rich in information that can be exploited by malicious entities or curious service providers to uncover user sensitive attributes beyond those disclosed intentionally and required for the purpose of the service or to directly identify a person. Besides the biometric information carried by eye movement data, research has also documented their correlation with multiple disorders and mental conditions, such as Alzheimer's [89],

schizophrenia [84, 113], Parkinson [109] bipolar disorder [66], mild cognitive impairment [207] multi sclerosis [49], Autism [24, 201], or psychosis [59], to name a few. Furthermore, pupil size is known to be an indicator of a person's interest in a scene [80] and a proxy for detecting cognitive load [107, 130]. Other recent works demonstrated that eye data can be used to infer gender and age, or even personality traits [18, 108]. Given the richness of eye data and the increased availability of consumer tracking devices and the advent of eye-gaze driven applications, there is a significant and imminent privacy threat potential [6].

The two main threats that endanger eye privacy are re-identification and attributes' inference.

5.4.3 Anonymization Techniques. We found three proposals to protect the privacy of eye movement data [26, 116, 182], all of them are guided by on differential privacy (DP). The general idea of differentially private algorithms is to add a certain amount of randomly generated noise to the original signal, so that it is difficult to say whether or not an individual contributed their data.

Noise Injection. Steil et al. [182] propose a DP-based technique to protect eye movement data collected while users read different types of document (comic, newspaper, textbook) in a VR setting. The utility goal is to accurately predict the type of document to provide enhanced features in the reader application. Additionally, the privacy goals are to avoid gender inferences from eye movement data and to protect against re-identification when the attacker has prior knowledge of a dataset including the target user eye data and identity. To achieve these goals, the exponential mechanism [54] is applied to a database of users' eye features by a trusted curator prior to its release. This sanitised database can be then used for training classifiers to provide the enhanced reader functionality. The experiments testing at various noise level show that utility with regard to document classification can be partly preserved (~55-70%) while reducing gender accuracy inference to the level of random guesses (~50%).

Based on Steil et al.'s dataset, Bozkir et al. [26] evaluate two types of DP-based perturbations, the standard Laplacian perturbation algorithm (LPA) [53] and the Fourier perturbation algorithm (FPA) [169]. They also propose a modification of the FPA algorithm that splits eye data in chunks before adding noise, in order to reduce temporal correlations, which is a source of reduced utility as more noise is required to protect privacy. With this modification, they obtain document type classification (comic, newspaper, textbook) results results similar tho those in [182] for the case of 50% gender classification, while adding more noise to the data (better privacy guarantee).

Liu et al. [116] present a DP-based solution to anonymize eye tracking data aggregated as a heatmap. A heatmap, or attentional landscape, is a popular method for visualizing eye movement data that represents aggregate fixations [52]. This means that the intensity of every pixel is adjusted relative to the number of fixations over that region. The privacy goal in this case is to protect individual gaze maps while preserving the utility of the aggregated heatmap. Their experiments with random selection and additive noise (Gaussian, Laplacian) show that Gaussian noise is the best option to obtain good privacy guarantees for the individuals' gaze maps without visually distorting the hotspots in the aggregated heatmap, i.e., keeping a certain utility.

5.4.4 Evaluation. The proposals by Steil et al. [182] and Bozkir et al. [26], measure the quality of their anonymization techniques for attribute inference protection using the classification accuracy metric for the main task and the attribute inference task. For the re-identification protection case, it is assumed that the attacker has previous knowledge of a database of users' eye data and their identities. To simulate this knowledge, they train the classifiers on the clean data and test them on the anonymized data , using also the accuracy metric to report privacy protection. Besides, these works also report the so called privacy loss parameter (or ϵ) from DP theory, which quantifies the maximum difference

between the data points of two individuals in the dataset. Furthermore, Bozkir et al. use the inverse of the normalized mean square error (NMSE) between the actual eye feature values and the perturbed ones as a utility metric. However, the interpretation and implications of these privacy loss and utility metrics are not developed.

Liu et al. [116] analyzed the privacy-utility tradeoff of anonymized heatmaps using the correlation coefficient (CC) and mean square error (MSE) of noisy heatmaps under different privacy levels (different values of ϵ). The CC and MSE give an idea of the similarity between the original and the anonymized heatmaps and the ϵ provides information about the privacy guarantee (the smaller, the better privacy). These metrics are accompanied by the visual representation of the noisy heatmap, in order to aid the relevant stakeholders in deciding what level of noise is acceptable for a given application.

Regarding datasets, Steil et al. [182] collect data from 20 participants (10 male, 10 female, aged 21-45) while reading documents using a VR headset. Each recording is divided into three sessions (reading a comic, newspaper, or textbook), lasting 30 minutes in total. They extract 52 eye movement features related to fixations, saccades, blinks, and pupil diameter. The dataset has been publicly released [3] by the authors and Bozkir et al. [26] use it as the basis to evaluate their proposal. In the heatmaps anonymization study, Liu et al. use a synthetic simulated dataset to illustrate their privacy analysis. Besides the technical privacy analysis, Steil et al. [182] is one of the few works considering user privacy concerns regarding behavioral data collection. They conduct a large scale user survey (with N=164 participants) to explore with whom, for which services, and to what extent users are willing to share their gaze data. Their report shows that people are uncomfortable with inferences (gender, race, sexual orientation) and would object to share their data if these attributes can be leaked. The results also show that people generally agree to share their eye tracking data if a governmental health agency or for research purposes, but would object to do so if the data owners are companies. These insights are a first step towards understanding user privacy awareness and privacy needs, but more work is required in this field to guide the design of user-centered privacy protective techniques for behavioral data.

5.5 Heartbeat

An electrocardiogram (ECG) is a graph of voltage over time that captures the electrical activities of cardiac muscle depolarization followed by repolarization during each heartbeat. Shown in Figure 9, the ECG graph of a normal beat is composed of a sequence of waves: a P-wave reflecting the atrial depolarization process, a QRS complex representing the ventricular depolarization process, and a T-wave denoting the ventricular repolarization. Other portions of the ECG signal encompass the PR, ST, and QT intervals [217].

As per the current screening and diagnostic practices, cardiologists review ECG data, find the right diagnosis and implement subsequent treatment plans such as a medication regime or the removal of a radiofrequency catheter. Nonetheless, the demand for highly accurate, automated heart-condition diagnoses has increased significantly, in part due to the new public health regulations of implementing more extensive screening processes as well as the adoption of ECG-enabled wearable devices.

It is well known that certain types of cardiovascular conditions, such as atrial fibrillation, have a wide and severe impact on public health, quality of life, and medical expenditures. The long-term ECG monitoring is a vital, non-invasive tool for detecting such conditions. For evident computational and intellectual property reasons, however, the analysis of such data is never conducted at the wearable device but at automated, machine-learning based systems typically

[3] https://www.mpi-inf.mpg.de/departments/computer-vision-and-machine-learning/research/visual-privacy/privacy-aware-eye-tracking-using-differential-privacy

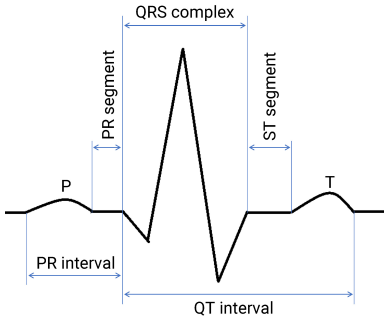

Fig. 9. Waveform of an ECG signal with normal cardiac cycle. Source: https://www.nottingham.ac.uk/nursing/practice/resources/cardiology/function/normal_duration.php.

hosted in hospitals or external service providers. This necessarily implies the transmission of ECG data from patients to non-fully trusted entities, which inevitably poses evident privacy risks.

However, the disclosure of sensitive data not only represents a threat to patients' privacy: it may also prompt a serious security risk to any biometric-authentication system that relies on those data. The advantage of ECG-data-based systems over other biometrics systems (like fingerprint, face or iris), though, is the intrinsic nature of ECGs and also their inherent indication of life, which make them very difficult to forge or steal [203]. Compared to fingerprint and facial recognition systems, where extra sensors —other than those required for medical monitoring purpose— are needed, ECGs are a more suitable choice in practical applications and have been shown to be extremely accurate in identification tasks [178].

Like other biometric systems applied to identification tasks, ECGs are typically converted into abstract, compressed representations, typically referred to as biometric templates[4], before the task is conducted[5]. Biometric-template methods can be classified depending on the exploited features of the ECG data. The most popular ones are fiducial-based, non-fiducial-based and hybrid methods [145]. On the one hand, fiducial-based techniques utilize characteristic points on the ECG signal to extract temporal, amplitude, envelope, slope and area features. Characteristic points are the locations that correspond to the peaks and boundaries of the P, QRS and T-waves of the ECG signal. On the other hand, the non-fiducial-based methods do not rely on the ECG characteristic points, and examples include autocorrelation coefficients, Fourier and wavelet transforms. Hybrid methods combine both fiducial-based and non-fiducial-based features.

Biometric templates are therefore an attempt to reduce data storage in identification services. In other type of services, ECG signals are expectedly compressed to allow efficient transmission and storage as well. As we shall elaborate later, techniques aimed to protect the transmission of ECG data will be classified depending on whether they are applied before or after compression.

5.5.1 Utility. ECG data find application in healthcare and biometrics systems, the latter being intended for identification and authentication, as discussed in the preliminaries of this section.

[4]As already mentioned in previous subsections, the functioning principle of biometric templates is that an original signal can be recovered from its template.
[5]Bear in mind that ECG signals are generally collected over long periods of time and at high resolutions. This leads to large volumes of data being collected. For example, for a sampling rate of 500 Hz and a data resolution of 8 bits per sample, a 24-h record amounts to about 43.2 Mbytes per channel.

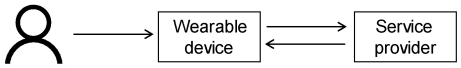

Fig. 10. Key entities in a scenario where ECG data are collected, processed and stored.

In healthcare, ECGs are utilized for remote diagnosis and in-home health monitoring. Typically, there is a stand-alone service or a complete e-health system where the service provider, in addition to offering a repository of personal medical data, may allow to remotely process such data. In any case, the aim is to provide real-time feedback to patients and hospitals, either as a warning of impending medical emergency or as a monitoring aid during physical exercises.

Although it is well known that ECG data may help diagnose a patient's physiological or pathological condition, other probably lesser-known inferences include cocaine use [86] and stress [157], which may be sensitive to the patient and obviously should be kept private. The fact that the very same time series data allows drawing both desirable inferences (i.e., for healthcare) and sensitive inferences (that need to be protected) poses a dilemma of great practical relevance.

5.5.2 Threat Space. Regardless of the application (i.e., identification, authentication or healthcare), ECGs are health data and, as such, are considered sensitive by data-protection regulations and need to be protected. Consider the case, for example, of a user who might see their insurance premium increased or suffer discrimination during a job application due to a medical condition inferred from their ECGs.

The general scenario where ECG data are collected, processed and stored is shown in Figure 10. The scenario is composed of three entities: a patient (in the case of healthcare applications) or user (in the case of identification and authentication applications); a wearable or internal[6] device collecting patient's ECG data; and an external entity that receives the data collected by the internal device, and processes and stores such information as a biometric template or in raw or compressed format, so as to provide a service.

Although the internal device is typically assumed to be trusted, both this and the external entity may be either trusted, partially trusted or fully untrusted. In the latter two cases, at the external entity the access of ECG data (including biometric templates) by unauthorized personnel poses an evident privacy threat and therefore should be prevented. As we shall elaborate in the coming subsections, privacy-protecting techniques will need to be put in place to allow only authorized personnel (e.g., medical personnel or cardiologists) to have access to ECG data or be able to reconstruct them from a biometric template.

Another aspect to consider within the spectrum of potential threats is the algorithm itself used by the service provider (e.g., a company or a hospital) to process ECG data. We have already mentioned that patients or users of the service could see their privacy compromised if their personal signal information or their biometric template was disclosed to a non-fully trusted-third party (not necessarily a hospital or doctor). However, protection is not only required by patients or users, but also by the service provider itself, which may not be willing to provide the end-user with its proprietary protocols because of fear of disclosing valuable intellectual property to third parties or compromising the basis for its service [111].

To conclude, a service provider might want to make the inferences model available to any health professional, e.g., through controlled queries, and/or like to publish anonymized ECG data as a means to crowdsourcing algorithmic development[7]. In both cases, the threats space would include the learned model and the released or published data.

[6] In the sense of within a patient or user's premises.
[7] The Netflix Prize [17] is probably the best-known example of collaborative-problem solving in the computer-science community.

5.5.3 Anonymization Techniques. Next we survey the most relevant privacy-protection techniques for ECG data.

Random Perturbation. As mentioned in the preliminaries, large volumes of data are collected in ECG-monitoring applications, and compression is very often needed for their transmission and storage. In this sense, Liu et al. [117] propose combining compression and encryption to provide privacy and confidentiality. Their proposal, however, differs from the typical compression-then-encryption approach, which may be problematic when untrusted network providers may conduct the compression task but do not have access to the private keys. The encryption-then-compression technique proposed by Liu et al. is composed of two steps. First, the ECG data, which are stored in a matrix, are multiplied by an orthogonal, randomly-generated key matrix. Then, singular-value decomposition (SVD) —a popular dimensionality-reduction technique— is applied to the encrypted data to provide compression.

Another approach based on compressive sensing (CS) [31] is proposed by Djelouat et al in [51]. CS is a signal processing technique that combines both sampling and compression through random projections. Building on this technique, the authors propose compressing the ECG signal by sampling it at the time of sensing. This reduces the need to even store the sensitive ECG data at the wearable device, thereby providing protection against that entity. The theoretical properties of this compression technique ensure that, under certain assumptions on the random projection, a good reconstruction of the original ECG signal can be obtained at the provider side.

Feature Removal. Kalai et al. [212] present a solution to secure the transmission of the ECG template between a wearable device and a service provider. In a first phase, the authors propose computing the discrete cosine transform (DCT) of the ECG signal's autocorrelation coefficients, and then removing those DCT coefficients with the lowest energy. The remaining DCT coefficients constitute the biometric template. In a second phase, two keys are obtained from the template. One is transmitted to the target application the user wishes to authenticate. The other functions as a private key, which is derived from the complete DCT already stored in the server.

A similar approach is presented by the same authors in [213] that uses a quantization step once the DCT-template is obtained. This latter approach is evaluated on the PTB dataset but no experimental comparison is conducted between the two proposed solutions.

Another similar proposal is [121], which decomposes the ECG signal into its wavelet transform, eliminates the low-frequency coefficients and reconstructs the ECG signal for release. At the provider side, only authorized personnel with access to a secret key (derived from the wavelet-transform template) is able to reconstruct the original ECG from the released, protected signal. To which extent these released data may safeguard patients' privacy is evaluated through the percentage root mean square difference (PRD), a simple and widely used distortion measure in ECG signal processing applications [126] that quantifies the difference between the original ECG and its protected version.

Utilizing the same transform, [185] proposes that, after the decomposition, the essential parts of the coefficients (which consists in the P, QRS and T signatures of the ECG) are treated differently, as follows. The non-essential parts of the signal are uploaded to a public repository in the clear, whereas the essential parts are encrypted and distributed among the healthcare experts in charge of analyzing patients' ECG data. In this process, the encrypted essential coefficients act as a key to reconstruct the original ECG, which can only accessed by authorized personnel.

Random Perturbation + Noise Injection. Although encryption based on the idea of CS can achieve a computational notion of secrecy through the random projection step, it has been shown this technique is vulnerable from an information-theoretic perspective [168]. To address this problem, Chou et al. [38] propose using principal component analysis and SVD on a CS scheme, where the ECG data is encrypted at the wearable sensor by adding signal-dependent noise. They

measure privacy as the mutual information between the original ECG signal and its encrypted version, and show that high classification accuracy can be achieved while providing privacy beyond computational secrecy.

Discrete Conversion + Noise Injection. Unlike the works surveyed previously, the goal of [214] is to publish suitable representations of ECG data with certain privacy guarantees. To do this, Zare-Mirakabad et al. propose converting ECG time series into symbolic representations over time. They use the popular Symbolic Aggregate approXimation (SAX) to replace continuous numerical values with strings of symbols (see Figure 11). With this new symbol representation, the proposed anonymization technique first builds an n-gram model from the complete time-series string, and then ensures that each n-gram has a minimum frequency of occurrence, similar to the k-anonymity criterion. To ensure this version of k-anonymity is satisfied over the string of symbols, the authors contemplate adding fake n-grams to the original string. Experimental results on the Eamonn Discord Dataset show that (a measure of) information loss is hardly affected for values of k up to 20.

Continuous Conversion + Random Perturbation. In [36] and subsequent work [203], the authors address the problem of making ECG-based biometric templates revocable, exactly as keys or passwords, a property they consider indispensable in order for ECGs to be used in practice. To enable template revocability, the common practice is to associate distinct templates with the same biometrics by perturbing them in a different manner. To protect user privacy, however, this process needs to ensure the recovery of the original biometric from its template is either infeasible or computationally hard.

Essentially, cancelable templates are obtained as random projections of a user's ECG data block. Unlike common approaches, however, [203] puts no restrictions on the generator matrix. Accordingly, the idea is that each realization of this matrix allows cancelling their corresponding templates. Reidentification is then conducted with the multiple-signal classification algorithm [19], reporting rates of over 95% in the Physikalisch Technische Bundesanstalt Database.

A distinct approach is [85], which proposes a template-free identification system to prevent any privacy issue from compromised or stolen templates. The system converts ECG-data into images through various spatial and temporal correlations methods and uses deep-learning techniques to train a classifier. The authors conduct experiments on the Pysikalisch-Technische Bundesanstalt database and report identification rates of over 90% with sampling rates of 1 000 Hz.

Continuous Conversion + Noise Injection. Sufi et al. [184] propose building templates of the waves P, QRS and T through cross-correlations of the ECG signal. Each of those templates are then obfuscated in a concatenated fashion with additive noise generated synthetically, so that the obfuscation of a wave serves as input to obfuscate the next wave. The upshot are noisy forms of the three waves and noisy templates thereof. All this information constitutes the key available to authorized personnel, who will be able to reconstruct the original ECG from the noisy version (which is shared or made publicly available by the patient or user themselves). Unauthorized personnel, per contra, will only have access to the noisy ECG signal, which, according to the authors, may prevent identity and attribute disclosure.

Chen et al. [37] tackle the problem of federated learning, where the goal is to train of a machine-learning classifier with ECG data distributed over a set of entities (e.g., health institutions). The authors assume the central server coordinating the learning process and updating the global model is untrusted and resorts to block-chain technology to address this issue. Differential privacy is the privacy model used to guarantee the privacy of entities' patients. Specifically, the authors rely on the common approach of adding noise to the local gradients, and address the asynchronous problem that arises when local gradients are missing or delayed in each iteration, by adopting the solution proposed in [219].

Experimental results on the MIT-BIH ECG Arrhythmia Database [136] show the classification performance over ten types of cardiac arrhythmia is around 20% in test error for $\varepsilon = 0.1$ and 600 iterations.

Huang et al. [88] propose an authentication system that protects the privacy of ECG templates in a database with differential privacy. The authors assume the interactive setting of this privacy notion, where an analyst queries the database to obtain ECG data. Specifically, the analyst is supposed to ask for the coefficients of a Legendre polynomial, that the anonymization system utilizes to fit and compress the ECG signal. Laplace noise is calibrated to the sensitivity of those coefficients and added to them, and the noisy response is returned to the analyst. The ε parameter of DP therefore regulates the trade-off between user privacy and authentication accuracy, the latter aspect depending on two sources of error: the polynomial fitting approximation and the injected noise. The authors evaluate the system in the MIT-BIH ECG and MIT-BIH Noise Strees databases, reporting decent authentication accuracy. However, they appear to misunderstand how the sensitivity of the coefficients is computed and therefore their results seem to have been obtained incorrectly.

Saleheen et al. [176] investigates if sensitive inferences from segments of time series data can be drawn by a dynamic Bayesian network adversary. The adversary is assumed to estimate a range of behavioral states about the user, including, for example, whether or not they are in a conversation, running, smoking and stress, at the time the data is gathered. When the adversary is likely to infer sensitive aspects of a user, the corresponding segments of data are substituted for most-plausible, non-sensitive data. To estimate the privacy provided by these substitutions of data, the authors propose a variation of the differential-privacy notion that bounds the information leaked resulting from the substitutions. In other words, the proposed metric ensures that the information leaked about a sensitive inference from a substituted segment is always bounded. Utility loss is, on the other hand, computed as the absolute difference between the probability of inference about each non-sensitive behavioral state from actual data, and the same probability from released data. Although experimental results show relatively small values of utility loss for $\varepsilon \in [0.05, 0.65]$, the proposed solution has two main limitations: first, protection is provided only for dynamic Bayesian network adversaries; and secondly, it assumes all time-series data are available beforehand, which precludes its application in real-time scenarios.

In [47], Delaney et al. investigate the ability of generative adversarial networks (GANs) to produce realistic medical time series data. Typically, the access to medical data is highly restricted due to its sensitive nature, which prevents communities from using this data for research or clinical training. The aim of this work is to generate synthetic ECG signals representative of normal ECG waveforms without concerns over privacy. On the one hand, the authors measure utility as maximum mean discrepancy (MMD) and dynamic time warping (DTW), two common approaches to estimate the dissimilarity between two probability distributions and two time series, respectively. On the other, user privacy is evaluated as the accuracy of a membership inference attack who strives to ascertain whether or not a user's data was used for training. Experimental results on MIT-BIH Arrythmia Database [136] show that MMD favours GANs that generate a diverse range of outputs, while DTW is more robust against training instability. Although the authors report low accuracy results for such inference attacks, it is unclear if their solution would protect against more recent, sophisticated [35] versions of those attacks.

5.5.4 Evaluation. The reviewed techniques measure how service functionality is degraded due to anonymization with common machine learning metrics like precision, recall and accuracy, and less frequently with the DTW and PRD quantities, which assess the similarity between original and protected time series. As for privacy, the level of protection is assessed through a variety notions and measures, including the accuracy of a membership inference attack, the ε parameter of differential privacy, the mutual information between the original ECG signal and its encrypted version,

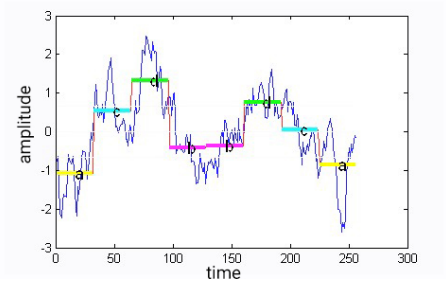

Fig. 11. A time series is converted into the string "acdbbdca". Source: https://cs.gmu.edu/~jessica/sax.htm.

the probability of correct inferences on sensitive attributes with and without protection, and through a notion similar to k-anonymity.

5.6 Brain Activity

Brainwaves are patterns of measurable electrical impulses emitted as a result of the interaction of billions of neurons inside the human brain. Since the first human electroencephalogram was recorded in 1924 [75], both the hardware devices to measure brain activity and the analysis techniques to process these signals have significantly improved. Current technologies to measure brainwaves can be classified as invasive and noninvasive methods. Invasive methods record signals within the cortex by directly implanting electrodes near the surface of the brain [96]. These methods are far too risky for usage under noncritical circumstances and only used in clinical applications. Instead, non-invasive methods are most frequently used and applicable to many areas other than the medical realm, such as brain-controlled interfaces. The most portable and commonly used of these techniques is electroencephalograpy (EEG), which records electrical activity through sensors placed on the scalp surface.

An EEG signal is a combination of different brainwaves occurring at different frequencies. Every type of wave carries different kinds of information, which can be used to gain insights about the current state of the brain [8]. Researchers have tried to identify certain mental states associated to each brainwave. Table 1 presents a summary of the most important wave types, their respecttive frequencies, their originating location in the brain, and their associated mental state.

Brain-computer interface (BCI) technologies mostly work on continuous EEG data recordings, i.e., time series data. But there are also many applications based on the extraction of time-locked brain variations that appear in reaction to external stimuli. These variations, called event related potentials (ERPs), are widely used to detect neurological diseases. In both cases, either using ERPs or a longer EEG series, features are computed for the brainwave data-driven application built on top. These features can belong to the time and/or frequency domain, and to one or multiple channels. Examples of commonly used features include Autoregressive coefficients, Fourier and Wavelet transforms.

5.6.1 Utility. The utility that should be preserved when processing brainwave data is highly dependent on the application. For clinical applications, for example, the raw information could be needed for a proper diagnosis or a safe brain controlled prosthesis. In these cases, regulations like the HIPAA Privacy Rule [11] are usually in place to protect personal identifiable information. When moving to other less regulated fields of application, the need for full raw EEG data is not necessarily justified. The most prominent EEG applications include user authentication, personalization of gaming experiences, and brain controlled-interfaces. In these cases, the utility to be preserved should be enough

Brain Wave Type	Freq. (Hz)	Originating Location in the Brain	Mental State
Gamma γ	30-100	Somatosensory cortex	Active information processing, strong response to visual stimuli [2]
Beta β	13-30	Both hemispheres, frontal lobe	Increased alertness, anxious thinking, focused attention
Alpha α	8-13	Posterior regions, both hemispheres; High amplitude waves	Resting, eyes closed, no attention [101]; Most dominant rhythm
Theta θ	4-8	No special location	Idling, dreaming, imagining, quiet focus, memory retrieval
Delta δ	0.5-4	Frontal regions; High amplitude waves	Dreamless and deep sleep, unconsciousness

Table 1. Overview of EEG brainwaves - based on [8] and [2].

to provide a useful application, i.e., recognize the user, offer personalized options and responsive interfaces all with a tolerable error that does not hamper the security and usability of the service.

5.6.2 Threat space. Brain activity is rich in information. It can be used to uniquely identify individuals given their unique characteristics and, in fact, several biometric systems based on brainwaves have been proposed [74]. Besides, the acquisition of EEG signals raises privacy issues because brainwaves correlate, among others, with our mental states, cognitive abilities, and medical conditions [186]. A third party in possession of neural data could try to make inferences of private attributes that were not intentionally disclosed by the user subscribing to its service, and thus non consented. Furthermore, if this entity has the ability to control the stimuli presented to the user when collecting their brainwave activity, such as the images shown in the computer screen, it could manipulate them to obtain private data. Martinovic et al. [127] where among the first to demonstrate the feasibility of these type of attacks. Focusing on users of low cost EEG readers, they successfully proved that, by manipulating the images presented to the users, their EEG signals could reveal private information about, e.g., bank cards, PIN numbers, area of living, or if the user knew a particular person. In another work, Frank et al. [64] show how to obtain private data from EEG recordings but, in this case, through subliminal stimuli (short duration images embedded in visual content) that cannot even be consciously detected by users. On the positive side, contrary to other behavioral traits like keystrokes or gait, brainwaves cannot be observed from the outside, which limits the possibility to misuse observed data to identify users without consent [105]. Overall, the two main threats that apply to brainwave data collected/processed by a third party service provider are re-identification and inference of private attributes. In the first case, the attack would consist of linking the brain data of the user to brain data collected by other service or available in public databases, gaining additional information about the user that can potentially be identifiable or reveal sensitive information. In the second case, the attack is oriented to uncover attributes correlated with the brainwave data, such as emotions, for which the user did not consent.

5.6.3 Anonymization Techniques. We found two works on brainwave data anonymization [129, 208], both of them targeting the privacy goal of avoiding sensitive attribute inferences, more specifically, being an alcoholic , through feature removal.

Feature removal. Matovu et al. [128] explore how to reduce the leakage of private information from EEG user authentication templates. They assume an insider type of attacker, such as an unscrupulous database administrator,

who misuses their privilege to maliciously exploit the templates. The attacker wants to infer, specifically, if the user associated with a template is an alcoholic. Their envisioned anonymization technique aims at concealing the alcoholism information while still providing good authentication accuracy. It is, therefore, an attribute protection mechanism. Conceptually, it lies on the hypothesis that different template designs (features, channels, frequencies) will have an impact on the amount of non-authentication information (emotions, health conditions) that can be inferred. The authors demonstrate this hypothesis by choosing two different templates and calculating the predictive capability to authenticate users and to determine their alcohol consumption behavior. One of the template designs shows a good trade-off between accuracy and alcoholism obfuscation, while the other template provides better accuracy at the expense of leaking alcohol consumption behavior. While these results support the hypothesis, the article does not propose a concrete and systematic methodology to design the templates.

In the same direction of feature selection, Yao et al. [208] propose the usage of Generative Adversarial Networks (GANs) [71] to filter sensitive information out of EEG data. Their goal is to reduce the possibility of inferring alcoholism while keeping the brain activity recordings useful to detect mental tasks, specifically to predict which visual stimulus the user is looking at. The GAN-based proposed filter involves deep neural networks that perform domain transformation, that is, translating EEGs from a source domain distribution X with both desired and privacy-related features to a target domain distribution Y with desired features only. Their results after applying the filtering technique show a significant reduction in the percentage of EEG sequences from alcoholic users that can be classified as such (from 90.6% to 0.6%). At the same time, the mental task classification accuracy does not drop significantly (4.2% less). However, the original mental task classifier accuracy was not strong before filtering the privacy-sensitive features and it remains to be studied if this technique would work in other classification scenarios.

5.6.4 Evaluation. The reviewed works, similar to the proposals for anonymizing gait, evaluate the quality of inference protection by comparing the prediction accuracy for the protected attribute before and after modifying the EEG data. The metrics used for this analysis are typical machine learning metrics, including accuracy, false positive rates, and false negative rates. Similarly, the loss of utility is evaluated by measuring the reduction in classification accuracy when using the original and anonymized EEG data.

Both works used the same publicly available dataset for evaluating their anonymization proposals, the SUNY medical dataset with EEG data of 25 alcoholic subjects and 25 control subjects while looking at visual stimuli [97, 143].

6 DISCUSSION

All reviewed behavioral biometric traits have in common that they are captured as a time-series tracking the change of the trait over time. Most traits, such as gait, hand motions, voice, and eye gaze are overt traits that can be observed from a distance and do not require the participation of the subject. These traits are often captured as a byproduct for other recordings, for example, video recordings. EEG and ECG on the other hand are secret traits that can mostly only be recorded by directly attaching sensors to the subject to measure them. Due to the missing requirement of user participation for the observable traits they are more prone to be abused for surveillance, or identity theft. Given that we, and others, upload/store a lot of info about ourselves, there is plenty of basis for making inferences. Therefore it is necessary to protect these traits more severely from being stolen or abused.

The utility of these traits is very diverse and is mostly unique to each trait and the application using it. It ranges from utilities such as the naturalness of a motion to the intelligibility of utterances.

Regarding their threat space, the traits are similar to each other because the instances they are recorded are increasing with the pervasiveness of digital capturing devices such as smartphones and wearables in our everyday life. Wearables are of especial interest as they are attached to the subject and can therefore allow continuous capture of behavioral data. As our literature review has shown all traits can be used for both identity and attribute inference, which then can be used in a wide variety of privacy threats such as surveillance, identity theft, or private attribute inference. The privacy goals, identity protection, and attribute protection are also the same for all the traits. However, voice has an additional privacy goal in which the content of the speech should be made unintelligible.

For the techniques (see Table 2) that we reviewed, we found that most of them fall into the category of continuous conversion, followed by feature removal and noise injection. Next are random perturbation and discrete conversion, with most discrete conversion methods aiming at template protection. Coarsening is the category with the least amount of methods. We observe several differences for the categories of our taxonomy, for the removal methods we find that the removal is not directly reversible, however, due to the high redundancy in behavioral biometric data it still might be possible to reconstruct the removed data. For the conversion methods, we often observe that the parameter space for the anonymizations is often rather small, making it possible that an attacker can link clear and anonymized data by brute forcing the parameters when the anonymization technique is known. In general, we find that the reversibility of conversion techniques should be evaluated. For noise injection techniques we find that the strong dependency both temporal and physiological a problem since they allow can be used to filter out the noise.

With regard to the techniques providing differential privacy, we have observed that none of them can be used continuously over time without completely compromising patient or user privacy. The reason lies in that the privacy budget is necessarily finite, which means, by the sequential composition property of differential privacy [131], that it will be consumed completely at some time instant. Surprisingly, this appears to be in contradiction to the intended use of most of the applications where differential privacy is guaranteed, namely, continuous monitoring in healthcare scenarios, and identification and authentication services (which clearly are not single-use services). In that respect, the use of related privacy notions intended for continuous observations (e.g., w-event differential privacy [99]) may come in handy.

We found the most anonymization methods for voice and the least for EEG. For the traits touch, thermal, lip-facial, and motion we could not find any methods. We made the observation that most methods do not manipulate the temporal aspect of their data. Notable exceptions are Hirose et al. [81] and Maiti et al. [123]. Since all traits result in time series data manipulating the temporal order or time differences between events could lead to some general anonymization techniques which work for multiple traits. For attribute protection we find anonymizing intrinsic attributes (e.g., age, sex) to be difficult as it is not clear which part of the behavioral data is relevant for these attributes. Further, we noticed a lack of even basic understanding of users' privacy awareness and concerns about behavioral privacy. These are necessary to design protection techniques that consider user needs and requirements.

We found that the evaluation methodology between the traits and methods is rather similar. In general, an inference/recognition system is being used on the clear and on the anonymized data and then the difference in accuracy is reported, often without retraining the inference system on the anonymized data. We find this methodology too simple as the underlying assumption is that the attacker is not aware of the anonymization. Besides training the recognition model on the anonymized data the evaluations should also consider an attacker that actively tries to reverse the anonymization and knows the anonymization technique and its parameters. To allow the comparison between multiple methods the attacker models should be made explicit and common, similar to attacker models in cryptography. Only a handful of papers compare their own methods to that of others and due to the differences in

attacker models and data sources, it is difficult to compare their results to one another. We also found that there are not many approaches [167, 215] to formalize the privacy of behavioral biometric anonymization methods and most of the evaluations rely on empirical privacy estimations. Another problem is that the evaluation methodology is too close to the recognition system evaluation methodology which seeks to infer persons in a large dataset with poor data quality, while an anonymization method should also work on a small group size with high data quality. We believe that the lack of available datasets (see Table 3) is one of the main problems which keeps the less researched behavioral biometric traits back.

Method \ Trait	Voice	Gait	Hand motion	Eye-Gaze	Brain activity	Heartbeat
continuous conversion	[92] [158] [180] [95] [3] [164] [13] [60] [100] [61] [1] [118] [119] [9] [181] [32]† [103]* [104]* [166]* [165]* [181]*	[7] [91] [81]‡	[122]			[36]† [203]† [85]† [184]* [37]* [88]* [176]* [47]*
discrete conversion	[153] [162] [163] [20]		[174] [112] [134] [198] [63]			[214]*
feature removal	[152] [150] [204] [216] [141] [142] [39]	[94]			[128] [208]	[212] [213] [121] [185]
coarsening			[123] [198]			
noise injection	[187] [78] [76] [146] [197]	[192] [193] [191] [129]	[133] [135]	[182] [26] [116]		
random perturbation	[151] [139]	[82]	[122] [72] [123] [198]			[117] [51] [38]*

Table 2. An overview of all found methods classified by trait and method. Papers that propose multiple methods can appear in multiple rows. Papers that combine multiple methods are marked the following: * plus noise injection, † plus random perturbation, ‡ plus discrete conversion.

7 CONCLUDING REMARKS

Anonymizing behavioral biometric data is an important task for protecting people's privacy. In our literature review, we found many different behavioral traits that need to be considered and developed a taxonomy to classify the anonymization techniques that can be applied to them by the type of data transformation they perform. While voice

Name	Participants	Published	Source	Trait
TIMIT	630	1993	[67]	Voice
Albayzin	164	1993	[138]	Voice
YOHO	137	1994	[30]	Voice
BioSecureID	400	2009	[62]	Voice
Billeb et al.	701	2014	[20]	Voice
Librispeech	1166	2015	[148]	Voice
RSR2015	300	2015	[110]	Voice
VoxCeleb	1251	2018	[140]	Voice
CASIA-B	124	2005	[220]	Gait
i3DPost	8	2009	[70]	Gait
BEHAVE	125	2010	[21]	Gait
OU-ISIR	200	2012	[125]	Gait
MCYT baseline corpus	330	2003	[147]	Hand motion
SVC2004	100	2004	[210]	Hand motion
GREYC	133	2009	[68]	Hand motion
MNIST	500	2012	[48]	Hand motion
Web-based keystroke	83	2012	[69]	Hand motion
SUNY EEG database	50	1999	[143]	Brain activity
MIT-BIH ECG Arrhythmia	47	1979	[136]	Heartbeat
MIT-BIH Noise Stress Test	2	1984	[137]	Heartbeat
Physikalisch Technische Bundesanstalt	290	1995	[25]	Heartbeat

Table 3. An overview of used behavioral biometric datasets.

anonymization is already a research field with many available solutions, most behavioral biometric traits only got little attention in the literature and therefore anonymizing them remains an open research question. We further found that most anonymization techniques are only evaluated rudimentarily with the assumption of a weak attacker. Improving the evaluation methodology is therefore another open research question. Lastly, we find that the temporal aspect of the data was mostly neglected, both for offering privacy for data streams and for anonymizing the data.

REFERENCES

[1] Alberto Abad, Alfonso Ortega, António Teixeira, Carmen García Mateo, Carlos D. Martínez Hinarejos, Fernando Perdigão, Fernando Batista, and Nuno Mamede (Eds.). 2016. *Advances in Speech and Language Technologies for Iberian Languages*. Lecture Notes in Computer Science, Vol. 10077. Springer International Publishing. https://doi.org/10.1007/978-3-319-49169-1

[2] Mohammed Abo-Zahhad, Sabah Mohammed Ahmed, and Sherif Nagib Abbas. 2015. State-of-the-art methods and future perspectives for personal recognition based on electroencephalogram signals. *IET Biometrics* 4, 3 (sep 2015), 179–190. https://doi.org/10.1049/iet-bmt.2014.0040

[3] Mohamed Abou-Zleikha, Zheng-Hua Tan, Mads Graesboll Christensen, and Soren Holdt Jensen. 2015. A discriminative approach for speaker selection in speaker de-identification systems. In *2015 23rd European Signal Processing Conference (EUSIPCO)*. IEEE, 2102–2106. https://doi.org/10.1109/eusipco.2015.7362755

[4] Richard A Abrams, David E Meyer, and Sylvan Kornblum. 1989. Speed and accuracy of saccadic eye movements: Characteristics of impulse variability in the oculomotor system. *Journal of Experimental Psychology: Human Perception and Performance* 15, 3 (1989), 529. https://doi.org/10.1037/0096-1523.15.3.529

[5] Christopher Ackad, Andrew Clayphan, Roberto Martinez Maldonado, and Judy Kay. 2012. Seamless and continuous user identification for interactive tabletops using personal device handshaking and body tracking. In *CHI '12 Extended Abstracts on Human Factors in Computing Systems*. ACM, 1775–1780. https://doi.org/10.1145/2212776.2223708

[6] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M. Redmiles. 2018. Ethics Emerging: the Story of Privacy and Security Perceptions in Virtual Reality. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association,

Baltimore, MD, 427–442. https://www.usenix.org/conference/soups2018/presentation/adams

[7] Prachi Agrawal and P. J. Narayanan. 2011. Person De-Identification in Videos. *IEEE Transactions on Circuits and Systems for Video Technology* 21, 3 (mar 2011), 299–310. https://doi.org/10.1109/tcsvt.2011.2105551

[8] Abdulaziz Almehmadi and Khalil El-Khatib. 2013. The state of the art in electroencephalogram and access control. In *2013 Third International Conference on Communications and Information Technology (ICCIT)*. IEEE, Beirut, Lebanon, 49–54. https://doi.org/10.1109/iccitechnology.2013.6579521

[9] Ranya Aloufi, Hamed Haddadi, and David Boyle. 2019. Emotionless: Privacy-Preserving Speech Analysis for Voice Assistants. arXiv:1908.03632 [cs.CR]

[10] Abdulaziz Alzubaidi and Jugal Kalita. 2016. Authentication of Smartphone Users Using Behavioral Biometrics. *IEEE Communications Surveys & Tutorials* 18, 3 (2016), 1998–2026. https://doi.org/10.1109/comst.2016.2537748

[11] HIPAA Compliance Assistance. 2003. Summary of the hipaa privacy rule. *Office for Civil Rights* (2003).

[12] A.Terry Bahill, Michael R. Clark, and Lawrence Stark. 1975. The main sequence, a tool for studying human eye movements. *Mathematical Biosciences* 24, 3-4 (jan 1975), 191–204. https://doi.org/10.1016/0025-5564(75)90075-9

[13] Fahimeh Bahmaninezhad, Chunlei Zhang, and John Hansen. 2018. Convolutional Neural Network Based Speaker De-Identification. In *Odyssey 2018 The Speaker and Language Recognition Workshop*. ISCA, 255–260. https://doi.org/10.21437/odyssey.2018-36

[14] Dustin Bales, Pablo A. Tarazaga, Mary Kasarda, Dhruv Batra, A. G. Woolard, J. D. Poston, and V. V. N. S Malladi. 2016. Gender Classification of Walkers via Underfloor Accelerometer Measurements. *IEEE Internet of Things Journal* 3, 6 (dec 2016), 1259–1266. https://doi.org/10.1109/jiot.2016.2582723

[15] Salil Partha Banerjee and Damon Woodard. 2012. Biometric Authentication and Identification Using Keystroke Dynamics: A Survey. *Journal of Pattern Recognition Research* 7, 1 (2012), 116–139. https://doi.org/10.13176/11.427

[16] BehavioSec. [n.d.]. Continuous Authentication Through Behavioral Biometrics. Webpage. https://www.behaviosec.com Accessed: 17.05.2019.

[17] James Bennet and Stan Lanning. 2007. The Netflix Prize. In *Proceedings of the KDD Cup Workshop 2007*. ACM, 3–6. http://www.cs.uic.edu/~liub/KDD-cup-2007/NetflixPrize-description.pdf

[18] Shlomo Berkovsky, Ronnie Taib, Irena Koprinska, Eileen Wang, Yucheng Zeng, Jingjie Li, and Sabina Kleitman. 2019. Detecting Personality Traits Using Eye-Tracking Data. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 1–12. https://doi.org/10.1145/3290605.3300451

[19] G. Bienvenu and L. Kopp. 1980. Adaptivity to background noise spatial coherence for high resolution passive methods. In *ICASSP '80. IEEE International Conference on Acoustics, Speech, and Signal Processing*, Vol. 5. Institute of Electrical and Electronics Engineers, 307–310. https://doi.org/10.1109/icassp.1980.1171029

[20] Stefan Billeb, Christian Rathgeb, Herbert Reininger, Klaus Kasper, and Christoph Busch. 2015. Biometric template protection for speaker recognition based on universal background models. *IET Biometrics* 4, 2 (jun 2015), 116–126. https://doi.org/10.1049/iet-bmt.2014.0031

[21] Scott Blunsden and RB Fisher. 2010. The BEHAVE video dataset: ground truthed video for multi-person behavior classification. *Annals of the BMVA* 4, 1-12 (2010), 4.

[22] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *2012 IEEE Symposium on Security and Privacy*. IEEE, 553–567. https://doi.org/10.1109/sp.2012.44

[23] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2015. Passwords and the evolution of imperfect authentication. *Commun. ACM* 58, 7 (jun 2015), 78–87. https://doi.org/10.1145/2699390

[24] Zillah Boraston and Sarah-Jayne Blakemore. 2007. The application of eye-tracking technology in the study of autism. *The Journal of Physiology* 581, 3 (jun 2007), 893–898. https://doi.org/10.1113/jphysiol.2007.133587

[25] Schnabel A. Bousseljot R, Kreiseler D. 1995. Nutzung der EKG-Signaldatenbank CARDIODAT der PTB über das Internet. *Biomedizinische Technik* 40, 1 (1995).

[26] Efe Bozkir, Onur Günlü, Wolfgang Fuhl, Rafael F. Schaefer, and Enkelejda Kasneci. 2020. Differential Privacy for Eye Tracking with Temporal Correlations. arXiv:2002.08972 [cs.CR]

[27] Attaullah Buriro, Zahid Akhtar, Bruno Crispo, and Filippo Del Frari. 2016. Age, Gender and Operating-Hand Estimation on Smart Mobile Devices. In *2016 International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, IEEE, 1–5. https://doi.org/10.1109/biosig.2016.7736910

[28] Tom Bäckström, Okko Räsänen, Abraham Zewoudie, and Pablo Pérez Zarazaga. [n.d.]. Introduction to Speech Processing. WebPage. https://wiki.aalto.fi/display/ITSP/ Accessed: 02.02.2021.

[29] W.M. Campbell, D.E Sturim, and D.A. Reynolds. 2006. Support vector machines using GMM supervectors for speaker verification. *IEEE Signal Processing Letters* 13, 5 (may 2006), 308–311. https://doi.org/10.1109/lsp.2006.870086

[30] Campbell, Joseph and Higgins, Alan. 1994. YOHO Speaker Verification Corpus. *Linguistic Data Consortium* (nov 1994). https://doi.org/10.35111/3WC3-N668

[31] Emmanuel J. Candes, Justin Romberg, and Terence Tao. 2006. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. *IEEE Transactions on Information Theory* 52, 2 (feb 2006), 489–509. https://doi.org/10.1109/tit.2005.862083

[32] Anne M. P. Canuto, Fernando Pintro, and Michael C. Fairhurst. 2014. An effective template protection method for face and voice cancellable identification. *International Journal of Hybrid Intelligent Systems* 11, 3 (2014), 157–166. https://doi.org/10.3233/HIS-140192

[33] Jagmohan Chauhan, Yining Hu, Suranga Seneviratne, Archan Misra, Aruna Seneviratne, and Youngki Lee. 2017. BreathPrint: Breathing acoustics-based user authentication. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 278–291.

https://doi.org/10.1145/3081333.3081355

[34] Jagmohan Chauhan, Suranga Seneviratne, Yining Hu, Archan Misra, Aruna Seneviratne, and Youngki Lee. 2018. Breathing-Based Authentication on Resource-Constrained IoT Devices using Recurrent Neural Networks. *Computer* 51, 5 (may 2018), 60–67. https://doi.org/10.1109/mc.2018.2381119

[35] Dingfan Chen, Ning Yu, Yang Zhang, and Mario Fritz. 2020. GAN-Leaks: A Taxonomy of Membership Inference Attacks against Generative Models. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. ACM. https://doi.org/10.1145/3372297.3417238

[36] Peng-Tzu Chen, Shun-Chi Wu, and Jui-Hsuan Hsieh. 2017. A cancelable biometric scheme based on multi-lead ECGs. In *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, 3497–3500. https://doi.org/10.1109/embc.2017.8037610

[37] Xuhui Chen, Xufei Wang, and Kun Yang. 2019. Asynchronous Blockchain-based Privacy-preserving Training Framework for Disease Diagnosis. In *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 5469–5473. https://doi.org/10.1109/bigdata47090.2019.9006173

[38] Ching-Yao Chou, En-Jui Chang, Huai-Ting Li, and An-Yeu Wu. 2018. Low-Complexity Privacy-Preserving Compressive Analysis Using Subspace-Based Dictionary for ECG Telemonitoring System. *IEEE Transactions on Biomedical Circuits and Systems* 12, 4 (aug 2018), 801–811. https://doi.org/10.1109/tbcas.2018.2828031

[39] Alice Cohen-Hadria, Mark Cartwright, Brian McFee, and Juan Pablo Bello. 2019. Voice Anonymization in Urban Sound Recordings. In *2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP)*. IEEE, 1–6. https://doi.org/10.1109/mlsp.2019.8918913

[40] Cristina Conati, Christina Merten, Saleema Amershi, and Kasia Muldner. 2007. Using eye-tracking data for high-level user modeling in adaptive interfaces. In *AAAI*. 1614–1617.

[41] Emiliano De Cristofaro. 2021. A Critical Overview of Privacy in Machine Learning. *IEEE Security & Privacy* 19, 4 (jul 2021), 19–27. https://doi.org/10.1109/msec.2021.3076443

[42] Antitza Dantcheva, Petros Elia, and Arun Ross. 2016. What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics. *IEEE Transactions on Information Forensics and Security* 11, 3 (mar 2016), 441–467. https://doi.org/10.1109/tifs.2015.2480381

[43] Maria Cecilia Teixeira de Carvalho Bruno, Maria Aparecida Constantino Vilela, and Carlos Alberto B. Mendes de Oliveira. 2013. Study on dermatoses and their prevalence in groups of confirmed alcoholic individuals in comparison to a non-alcoholic group of individuals. *Anais Brasileiros de Dermatologia* 88, 3 (jun 2013), 368–375. https://doi.org/10.1590/abd1806-4841.20131829

[44] Ana Lígia Silva de Lima, Luc J. W. Evers, Tim Hahn, Lauren Bataille, Jamie L. Hamilton, Max A. Little, Yasuyuki Okuma, Bastiaan R. Bloem, and Marjan J. Faber. 2017. Freezing of gait and fall detection in Parkinson's disease using wearable sensors: a systematic review. *Journal of Neurology* 264, 8 (mar 2017), 1642–1654. https://doi.org/10.1007/s00415-017-8424-0

[45] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports* 3, 1 (mar 2013), 1376. https://doi.org/10.1038/srep01376

[46] Najim Dehak, Patrick J Kenny, Réda Dehak, Pierre Dumouchel, and Pierre Ouellet. 2011. Front-End Factor Analysis for Speaker Verification. *IEEE Transactions on Audio, Speech, and Language Processing* 19, 4 (may 2011), 788–798. https://doi.org/10.1109/tasl.2010.2064307

[47] Anne Marie Delaney, Eoin Brophy, and Tomas E. Ward. 2019. Synthesis of Realistic ECG using Generative Adversarial Networks. arXiv:1909.09150 [eess.SP]

[48] Li Deng. 2012. The MNIST Database of Handwritten Digit Images for Machine Learning Research [Best of the Web]. *IEEE Signal Processing Magazine* 29, 6 (nov 2012), 141–142. https://doi.org/10.1109/msp.2012.2211477

[49] Joy Derwenskus, Janet C Rucker, Alessandro Serra, John S Stahl, Deborah L Downey, Nancy L Adams, and R John Leigh. 2005. Abnormal Eye Movements Predict Disability in MS: Two-Year Follow-Up. *Annals of the New York Academy of Sciences* 1039, 1 (apr 2005), 521–523. https://doi.org/10.1196/annals.1325.058

[50] Clemens Deuser, Steffen Passmann, and Thorsten Strufe. 2020. Browsing Unicity: On the Limits of Anonymizing Web Tracking Data. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 279–292. https://doi.org/10.1109/sp40000.2020.00018

[51] Hamza Djelouat, Xiaojun Zhai, Mohamed Al Disi, Abbes Amira, and Faycal Bensaali. 2018. System-on-Chip Solution for Patients Biometric: A Compressive Sensing-Based Approach. *IEEE Sensors Journal* 18, 23 (dec 2018), 9629–9639. https://doi.org/10.1109/jsen.2018.2871411

[52] Andrew T. Duchowski. 2017. *Eye Tracking Methodology*. Springer International Publishing. https://doi.org/10.1007/978-3-319-57883-5

[53] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. 2017. Calibrating Noise to Sensitivity in Private Data Analysis. *Journal of Privacy and Confidentiality* 7, 3 (may 2017), 17–51. https://doi.org/10.29012/jpc.v7i3.405

[54] Cynthia Dwork and Aaron Roth. 2013. The Algorithmic Foundations of Differential Privacy. *Foundations and Trends® in Theoretical Computer Science* 9, 3-4 (2013), 211–407. https://doi.org/10.1561/0400000042

[55] Cynthia Dwork, Adam Smith, Thomas Steinke, and Jonathan Ullman. 2017. Exposed! A Survey of Attacks on Private Data. *Annual Review of Statistics and Its Application* 4, 1 (mar 2017), 61–84. https://doi.org/10.1146/annurev-statistics-060116-054123

[56] Simon Eberz, Giulio Lovisotto, Andrea Patane, Marta Kwiatkowska, Vincent Lenders, and Ivan Martinovic. 2018. When Your Fitness Tracker Betrays You: Quantifying the Predictability of Biometric Features Across Contexts. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, IEEE, 889–905. https://doi.org/10.1109/sp.2018.00053

[57] Khaled El Emam, Elizabeth Jonker, Luk Arbuckle, and Bradley Malin. 2011. A Systematic Review of Re-Identification Attacks on Health Data. *PLoS ONE* 6, 12 (dec 2011), e28071. https://doi.org/10.1371/journal.pone.0028071

[58] Fatih Ertam. 2019. An effective gender recognition approach using voice data via deeper LSTM networks. *Applied Acoustics* 156 (dec 2019), 351–358. https://doi.org/10.1016/j.apacoust.2019.07.033

[59] Ulrich Ettinger, Veena Kumari, Xavier A. Chitnis, Philip J. Corr, Trevor J. Crawford, Dominic G. Fannon, Séamus O'Ceallaigh, Alex L. Sumich, Victor C. Doku, and Tonmoy Sharma. 2004. Volumetric Neural Correlates of Antisaccade Eye Movements in First-Episode Psychosis. *American Journal of Psychiatry* 161, 10 (oct 2004), 1918–1921. https://doi.org/10.1176/ajp.161.10.1918

[60] Fuming Fang, Xin Wang, Junichi Yamagishi, Isao Echizen, Massimiliano Todisco, Nicholas Evans, and Jean-Francois Bonastre. 2019. Speaker Anonymization Using X-vector and Neural Waveform Models. *10th ISCA Speech Synthesis Workshop* (sep 2019). https://doi.org/10.21437/ssw.2019-28

[61] Marcos Faundez-Zanuy, Enric Sesa-Nogueras, and Stefano Marinozzi. 2015. Speaker identification experiments under gender De-identification. In *2015 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 1–6. https://doi.org/10.1109/ccst.2015.7389702

[62] J. Fierrez, J. Galbally, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, D. Ramos, D. T. Toledano, J. Gonzalez-Rodriguez, J. A. Siguenza, J. Garrido-Salas, E. Anguiano, G. Gonzalez de Rivera, R. Ribalda, M. Faundez-Zanuy, J. A. Ortega, V. Cardeñoso-Payo, A. Viloria, C. E. Vivaracho, Q. I. Moro, J. J. Igarza, J. Sanchez, I. Hernaez, C. Orrite-Uruñuela, F. Martinez-Contreras, and J. J. Gracia-Roche. 2009. BiosecurID: a multimodal biometric database. *Pattern Analysis and Applications* 13, 2 (feb 2009), 235–246. https://doi.org/10.1007/s10044-009-0151-4

[63] Lucas Silva Figueiredo, Benjamin Livshits, David Molnar, and Margus Veanes. 2016. Prepose: Privacy, Security, and Reliability for Gesture-Based Programming. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 122–137. https://doi.org/10.1109/sp.2016.16

[64] Mario Frank, Tiffany Hwu, Sakshi Jain, Robert Knight, Ivan Martinovic, Prateek Mittal, Daniele Perito, and Dawn Song. 2017. Subliminal Probing for Private Information via EEG-Based BCI Devices. arXiv:1312.6052 [cs.CR]

[65] Bence Galai and Csaba Benedek. 2015. Feature selection for Lidar-based gait recognition. In *2015 International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM)*. IEEE, 1–5. https://doi.org/10.1109/iwcim.2015.7347076

[66] Ana García-Blanco, Ladislao Salmerón, Manuel Perea, and Lorenzo Livianos. 2014. Attentional biases toward emotional images in the different episodes of bipolar disorder: An eye-tracking study. *Psychiatry Research* 215, 3 (mar 2014), 628–633. https://doi.org/10.1016/j.psychres.2013.12.039

[67] J. Garofolo, Lori Lamel, W. Fisher, Jonathan Fiscus, D. Pallett, N. Dahlgren, and V. Zue. 1992. TIMIT Acoustic-phonetic Continuous Speech Corpus. *Linguistic Data Consortium* (Nov. 1992).

[68] Romain Giot, Mohamad El-Abed, and Christophe Rosenberger. 2009. GREYC keystroke: A benchmark for keystroke dynamics biometric systems. In *2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*. IEEE, 1–6. https://doi.org/10.1109/btas.2009.5339051

[69] Romain Giot, Mohamad El-Abed, and Christophe Rosenberger. 2012. Web-Based Benchmark for Keystroke Dynamics Biometric Systems: A Statistical Analysis. In *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 11–15. https://doi.org/10.1109/iih-msp.2012.10

[70] Nikolaos Gkalelis, Hansung Kim, Adrian Hilton, Nikos Nikolaidis, and Ioannis Pitas. 2009. The i3DPost Multi-View and 3D Human Action/Interaction Database. In *2009 Conference for Visual Media Production*. IEEE, IEEE, 159–168. https://doi.org/10.1109/cvmp.2009.19

[71] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2020. Generative adversarial networks. *Commun. ACM* 63, 11 (oct 2020), 139–144. https://doi.org/10.1145/3422622

[72] Yuuki Goubaru, Yasushi Yamazaki, Takeru Miyazaki, and Tetsushi Ohki. 2014. A consideration on a common template-based biometric cryptosystem using on-line signatures. In *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)*. IEEE, 131–135. https://doi.org/10.1109/gcce.2014.7031229

[73] Erin Griffiths, Salah Assana, and Kamin Whitehouse. 2018. Privacy-preserving Image Processing with Binocular Thermal Cameras. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 4 (jan 2018), 1–25. https://doi.org/10.1145/3161198

[74] Qiong Gui, Maria V. Ruiz-Blondet, Sarah Laszlo, and Zhanpeng Jin. 2019. A Survey on Brain Biometrics. *Comput. Surveys* 51, 6 (feb 2019), 1–38. https://doi.org/10.1145/3230632

[75] Lindsay F Haas. 2003. Hans Berger (1873-1941), Richard Caton (1842-1926), and electroencephalography. *Journal of Neurology, Neurosurgery & Psychiatry* 74, 1 (jan 2003), 9–9. https://doi.org/10.1136/jnnp.74.1.9

[76] Jihun Hamm. 2017. Enhancing utility and privacy with noisy minimax filters. In *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 6389–6393. https://doi.org/10.1109/icassp.2017.7953386

[77] Katarzyna Harezlak and Pawel Kasprowski. 2018. Application of eye tracking in medicine: A survey, research issues and challenges. *Computerized Medical Imaging and Graphics* 65 (apr 2018), 176–190. https://doi.org/10.1016/j.compmedimag.2017.04.006

[78] Kei Hashimoto, Junichi Yamagishi, and Isao Echizen. 2016. Privacy-preserving sound to degrade automatic speaker verification performance. In *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 5500–5504. https://doi.org/10.1109/icassp.2016.7472729

[79] Jane Henriksen-Bulmer and Sheridan Jeary. 2016. Re-identification attacks—A systematic literature review. *International Journal of Information Management* 36, 6 (dec 2016), 1184–1192. https://doi.org/10.1016/j.ijinfomgt.2016.08.002

[80] Eckhard H Hess and James M Polt. 1960. Pupil Size as Related to Interest Value of Visual Stimuli. *Science* 132, 3423 (aug 1960), 349–350. https://doi.org/10.1126/science.132.3423.349

[81] Yuki Hirose, Kazuaki Nakamura, Naoko Nitta, and Noboru Babaguchi. 2019. Anonymization of Gait Silhouette Video by Perturbing Its Phase and Shape Components. In *2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*. IEEE, 1679–1685. https://doi.org/10.1109/apsipaasc47483.2019.9023196

[82] Thang Hoang, Deokjai Choi, and Thuc Nguyen. 2015. Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. *International Journal of Information Security* 14, 6 (jan 2015), 549–560. https://doi.org/10.1007/s10207-015-0273-1

[83] Giles Hogben. 2010. ENISA Briefing: Behavioural Biometrics. *Computational Intelligence* (2010).

[84] Philip S Holzman, Leonard R Proctor, and Dominic W Hughes. 1973. Eye-Tracking Patterns in Schizophrenia. *Science* 181, 4095 (jul 1973), 179–181. https://doi.org/10.1126/science.181.4095.179

[85] Pei-Lun Hong, Jyun-Ya Hsiao, Chi-Hsun Chung, Yao-Min Feng, and Shun-Chi Wu. 2019. ECG Biometric Recognition: Template-Free Approaches Based on Deep Learning. In *2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, 2633–2636. https://doi.org/10.1109/embc.2019.8856916

[86] Syed Monowar Hossain, Amin Ahsan Ali, Md. Mahbubur Rahman, Emre Ertine David Epstein, Ashley Kennedy, Kenzie Preston, Annie Umbricht, Yixin Chen, and Santosh Kumar. 2014. Identifying drug (cocaine) intake events from acute physiological response in the presence of free-living physical activity. In *IPSN-14 Proceedings of the 13th International Symposium on Information Processing in Sensor Networks (IPSN '14)*. IEEE, 71–82. https://doi.org/10.1109/ipsn.2014.6846742

[87] Jin Huafeng and Wang Shuo. 2017. Voice-based determination of physical and emotional characteristics of users. U.S. Patent 10 096 319B1.

[88] Pei Huang, Linke Guo, Ming Li, and Yuguang Fang. 2019. Practical Privacy-Preserving ECG-Based Authentication for IoT-Based Healthcare. *IEEE Internet of Things Journal* 6, 5 (oct 2019), 9200–9210. https://doi.org/10.1109/jiot.2019.2929087

[89] J Thomas Hutton, JA Nagel, and Ruth B Loewenson. 1984. Eye tracking dysfunction in Alzheimer-type dementia. *Neurology* 34, 1 (jan 1984), 99–99. https://doi.org/10.1212/wnl.34.1.99

[90] Michiko Inoue, Masashi Nishiyama, and Yoshio Iwai. 2020. Gender Classification using the Gaze Distributions of Observers on Privacy-protected Training Images. In *Proceedings of the 15th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*. SCITEPRESS - Science and Technology Publications, 149–156. https://doi.org/10.5220/0008876101490156

[91] M. Ivasic-Kos, A. Iosifidis, A. Tefas, and I. Pitas. 2014. Person de-identification in activity videos. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 1294–1299. https://doi.org/10.1109/mipro.2014.6859767

[92] Qin Jin, Arthur R. Toth, Tanja Schultz, and Alan W. Black. 2009. Voice convergin: Speaker de-identification by voice transformation. In *2009 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 3909–3912. https://doi.org/10.1109/icassp.2009.4960482

[93] I. Joe Louis Paul, S. Sasirekha, S. Uma Maheswari, K. A. M. Ajith, S. M. Arjun, and S. Athesh Kumar. 2019. Eye gaze tracking-based adaptive e-learning for enhancing teaching and learning in virtual classrooms. In *Information and Communication Technology for Competitive Strategies*. Springer, 165–176.

[94] Théo Jourdan, Antoine Boutet, and Carole Frindel. 2018. Toward privacy in IoT mobile devices for activity recognition. In *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. ACM, 155–165. https://doi.org/10.1145/3286978.3287009

[95] Tadej Justin, Vitomir Struc, Simon Dobrisek, Bostjan Vesnicer, Ivo Ipsic, and France Mihelic. 2015. Speaker de-identification using diphone recognition and speech synthesis. In *2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*. IEEE, 1–7. https://doi.org/10.1109/fg.2015.7285021

[96] E. Grace Mary Kanaga, R. Muthu Kumaran, M. Hema, R. Gowri Manohari, and Tina Anu Thomas. 2017. An experimental investigations on classifiers for Brain Computer Interface (BCI) based authentication. In *2017 International Conference on Trends in Electronics and Informatics (ICEI)*. IEEE, 1–6. https://doi.org/10.1109/icoei.2017.8300873

[97] Nader Karamzadeh, Yasaman Ardeshirpour, Matthew Kellman, Fatima Chowdhry, Afrouz Anderson, David Chorlian, Edward Wegman, and Amir Gandjbakhche. 2015. Relative brain signature: a population-based feature extraction procedure to identify functional biomarkers in the brain of alcoholics. *Brain and Behavior* 5, 7 (may 2015), e00335. https://doi.org/10.1002/brb3.335

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

[99] Georgios Kellaris, Stavros Papadopoulos, Xiaokui Xiao, and Dimitris Papadias. 2014. Differentially private event sequences over infinite streams. *Proceedings of the VLDB Endowment* 7, 12 (aug 2014), 1155–1166. https://doi.org/10.14778/2732977.2732989

[100] Gokce Keskin, Tyler Lee, Cory Stephenson, and Oguz H. Elibol. 2019. Measuring the Effectiveness of Voice Conversion on Speaker Identification and Automatic Speech Recognition Systems. arXiv:1905.12531 [eess.AS]

[101] W Khalifa, A Salem, and M Roushdy. 2012. A Survey of EEG Based User Authentication Schemes. In *The 8th International Conference on INFOrmatics and Systems (INFOS2012)*. 55–60.

[102] Barbara Kitchenham. 2004. *Procedures for performing systematic reviews*. Technical Report TR/SE-0401. Keele University, Keele, UK.

[103] Kazuhiro Kondo, Tomohiro Komiyama, and Shintaro Kashiwada. 2013. Towards Gender-Dependent Babble Maskers for Speech Privacy Protection. In *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 275–278. https://doi.org/10.1109/iih-msp.2013.77

[104] Kazuhiro Kondo and Hiroki Sakurai. 2014. Gender-Dependent Babble Maskers Created from Multi-speaker Speech for Speech Privacy Protection. In *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 251–254. https://doi.org/10.1109/iih-msp.2014.69

[105] Belal Korany, Chitra R. Karanam, Hong Cai, and Yasamin Mostofi. 2019. XModal-ID: Using WiFi for Through-Wall Person Identification from Candidate Video Footage. In *The 25th Annual International Conference on Mobile Computing and Networking*. ACM, 1–15. https://doi.org/10.1145/3300061.3345437

[106] M. Kosinski, D. Stillwell, and T. Graepel. 2013. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences* 110, 15 (mar 2013), 5802–5805. https://doi.org/10.1073/pnas.1218772110

[107] Krzysztof Krejtz, Andrew T. Duchowski, Anna Niedzielska, Cezary Biele, and Izabela Krejtz. 2018. Eye tracking cognitive load using pupil diameter and microsaccades with fixed gaze. *PLOS ONE* 13, 9 (sep 2018), e0203629. https://doi.org/10.1371/journal.pone.0203629

[108] Jacob Leon Kröger, Otto Hans-Martin Lutz, and Florian Müller. 2020. What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking. In *Privacy and Identity Management. Data for Better Living: AI and Privacy*. Springer International Publishing, 226–241. https://doi.org/10.1007/978-3-030-42504-3_15

[109] Craig A Kuechenmeister, Patrick H Linton, Thelma V Mueller, and Hilton B White. 1977. Eye Tracking in Relation to Age, Sex, and Illness. *Archives of General Psychiatry* 34, 5 (may 1977), 578–579. https://doi.org/10.1001/archpsyc.1977.01770170088008

[110] Anthony Larcher, Kong Aik Lee, Bin Ma, and Haizhou Li. 2012. The RSR2015: Database for text-dependent speaker verification using multiple pass-phrases. *13th Annual Conference of the International Speech Communication Association 2012, INTERSPEECH 2012* 2 (Jan. 2012), 1578–1581.

[111] Riccardo Lazzeretti, Jorge Guajardo, and Mauro Barni. 2012. Privacy preserving ECG quality evaluation. In *Proceedings of the on Multimedia and security - MM&Sec '12 (MM&Sec '12)*. ACM Press, 165–174. https://doi.org/10.1145/2361407.2361435

[112] Juho Leinonen, Petri Ihantola, and Arto Hellas. 2017. Preventing Keystroke Based Identification in Open Data Sets. In *Proceedings of the Fourth (2017) ACM Conference on Learning @ Scale*. ACM, 101–109. https://doi.org/10.1145/3051457.3051458

[113] Deborah L. Levy, Anne B. Sereno, Diane C. Gooding, and Gilllian A. O'Driscoll. 2010. Eye Tracking Dysfunction in Schizophrenia: Characterization and Pathophysiology. In *Behavioral Neurobiology of Schizophrenia and Its Treatment*. Springer, 311–347. https://doi.org/10.1007/7854_2010_60

[114] Yunji Liang, Sagar Samtani, Bin Guo, and Zhiwen Yu. 2020. Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective. *IEEE Internet of Things Journal* 7, 9 (sep 2020), 9128–9143. https://doi.org/10.1109/jiot.2020.3004077

[115] Jae Lim and A. Oppenheim. 1978. All-pole modeling of degraded speech. *IEEE Transactions on Acoustics, Speech, and Signal Processing* 26, 3 (jun 1978), 197–210. https://doi.org/10.1109/tassp.1978.1163086

[116] Ao Liu, Lirong Xia, Andrew Duchowski, Reynold Bailey, Kenneth Holmqvist, and Eakta Jain. 2019. Differential privacy for eye-tracking data. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*. ACM, 1–10. https://doi.org/10.1145/3314111.3319823

[117] Ting Yu Liu, Kuan Jen Lin, and Hsi Chun Wu. 2018. ECG Data Encryption Then Compression Using Singular Value Decomposition. *IEEE Journal of Biomedical and Health Informatics* 22, 3 (may 2018), 707–713. https://doi.org/10.1109/jbhi.2017.2698498

[118] Paula Lopez-Otero, Carmen Magariños, Laura Docio-Fernandez, Eduardo Rodriguez-Banga, Daniel Erro, and Carmen Garcia-Mateo. 2017. Influence of speaker de-identification in depression detection. *IET Signal Processing* 11, 9 (dec 2017), 1023–1030. https://doi.org/10.1049/iet-spr.2016.0731

[119] Carmen Magariños, Paula Lopez-Otero, Laura Docio-Fernandez, Eduardo Rodriguez-Banga, Daniel Erro, and Carmen Garcia-Mateo. 2017. Reversible speaker de-identification using pre-trained transformation functions. *Computer Speech & Language* 46 (nov 2017), 36–52. https://doi.org/10.1016/j.csl.2017.05.001

[120] Ahmed Mahfouz, Tarek M. Mahmoud, and Ahmed Sharaf Eldin. 2017. A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications* 37 (dec 2017), 28–37. https://doi.org/10.1016/j.jisa.2017.10.002

[121] Seedahmed S. Mahmoud. 2016. A generalised wavelet packet-based anonymisation approach for ECG security application. *Security and Communication Networks* 9, 18 (dec 2016), 6137–6147. https://doi.org/10.1002/sec.1762

[122] Emanuele Maiorana, Patrizio Campisi, and Alessandro Neri. 2011. Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system. In *2011 IEEE International Systems Conference*. IEEE, 495–500. https://doi.org/10.1109/syscon.2011.5929064

[123] Anindya Maiti, Oscar Armbruster, Murtuza Jadliwala, and Jibo He. 2016. Smartwatch-Based Keystroke Inference Attacks and Context-Aware Protection Mechanisms. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. ACM, 795–806. https://doi.org/10.1145/2897845.2897905

[124] Päivi Majaranta and Andreas Bulling. 2014. Eye Tracking and Eye-Based Human–Computer Interaction. In *Human–Computer Interaction Series*. Springer London, 39–65. https://doi.org/10.1007/978-1-4471-6392-3_3

[125] Yasushi Makihara, Hidetoshi Mannami, Akira Tsuji, Md. Altab Hossain, Kazushige Sugiura, Atsushi Mori, and Yasushi Yagi. 2012. The OU-ISIR Gait Database Comprising the Treadmill Dataset. *IPSJ Transactions on Computer Vision and Applications* 4 (Apr. 2012), 53–62. https://doi.org/10.2197/ipsjtcva.4.53

[126] M. Sabarimalai Manikandan and S. Dandapat. 2008. ECG Distortion Measures and their Effectiveness. In *2008 First International Conference on Emerging Trends in Engineering and Technology*. IEEE, 705–710. https://doi.org/10.1109/icetet.2008.248

[127] Ivan Martinovic, Doug Davies, Mario Frank, Daniele Perito, Tomas Ros, and Dawn Song. 2012. On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. In *21st USENIX Security Symposium (USENIX Security 12)*. USENIX Association, Bellevue, WA, 143–158. https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/martinovic

[128] Richard Matovu and Abdul Serwadda. 2016. Your substance abuse disorder is an open secret! Gleaning sensitive personal information from templates in an EEG-based authentication system. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, IEEE, 1–7. https://doi.org/10.1109/btas.2016.7791210

[129] Richard Matovu, Abdul Serwadda, David Irakiza, and Isaac Griswold-Steiner. 2018. Jekyll and Hyde: On The Double-Faced Nature of Smart-Phone Sensor Noise Injection. In *2018 International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, 1–6. https://doi.org/10.23919/biosig.2018.8553043

[130] Gerald Matthews, W Middleton, Bernard Gilmartin, and Mark A Bullimore. 1991. Pupillary diameter and cognitive load. *Journal of Psychophysiology* (1991).

[131] Frank D. McSherry. 2009. Privacy Integrated Queries: An Extensible Platform for Privacy-preserving Data Analysis. In *Proceedings of the 2009 ACM SIGMOD International Conference on Management of data*. ACM, 19–30. https://doi.org/10.1145/1559845.1559850

[132] Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou. 2015. Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys & Tutorials* 17, 3 (2015), 1268–1293. https://doi.org/10.1109/comst.2014.2386915

[133] Denis Migdal and Christophe Rosenberger. 2019. Keystroke Dynamics Anonymization System. In *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications*. SCITEPRESS - Science and Technology Publications, 448–455. https://doi.org/10.5220/0007923804480455

[134] Denis Migdal and Christophe Rosenberger. 2019. My Behavior is my Privacy & Secure Password !. In *2019 International Conference on Cyberworlds (CW)*. IEEE, 299–307. https://doi.org/10.1109/cw.2019.00056

[135] John V. Monaco and Charles C. Tappert. 2017. Obfuscating Keystroke Time Intervals to Avoid Identification and Impersonation. arXiv:1609.07612 [cs.CR]

[136] G.B. Moody and R.G. Mark. 1990. The MIT-BIH Arrhythmia Database on CD-ROM and software for use with it. In *[1990] Proceedings Computers in Cardiology*. IEEE Comput. Soc. Press, 185–188. https://doi.org/10.1109/cic.1990.144205

[137] G. B. Moody and Mark R. G. Muldrow, W. E. 1990. A noise stress test for arrhythmia detectors. *Computers in Cardiology* 11 (1990), 381–384.

[138] Asunción Moreno, Dolors Poch, Antonio Bonafonte, Eduardo Lleida, Joaquim Llisterri, José Mariño, and Climent Nadeu. 1993. Albayzin speech database: Design of the phonetic corpus. *Proc. Eurospeech* 1.

[139] Aymen Mtibaa, Dijana Petrovska-Delacretaz, and Ahmed Ben Hamida. 2018. Cancelable speaker verification system based on binary Gaussian mixtures. In *2018 4th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*. IEEE, 1–6. https://doi.org/10.1109/atsip.2018.8364513

[140] Arsha Nagrani, Joon Son Chung, and Andrew Zisserman. 2017. VoxCeleb: A Large-Scale Speaker Identification Dataset, In Interspeech 2017. *CoRR* abs/1706.08612. https://doi.org/10.21437/interspeech.2017-950

[141] Alexandru Nelus and Rainer Martin. 2018. Gender Discrimination Versus Speaker Identification Through Privacy-Aware Adversarial Feature Extraction. In *Speech Communication; 13th ITG-Symposium*.

[142] Alexandru Nelus and Rainer Martin. 2019. Privacy-aware Feature Extraction for Gender Discrimination versus Speaker Identification. In *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 671–674. https://doi.org/10.1109/icassp.2019.8682394

[143] SUNY Downstate Medical Center Neurodynamics Laboratory. 1999. EEG Database. http://kdd.ics.uci.edu/databases/eeg/eeg.data.html

[144] Nymi. [n.d.]. Always On Authantication. Webpage. https://nymi.com/ Accessed: 01.06.2019.

[145] Ikenna Odinaka, Po-Hsiang Lai, Alan D. Kaplan, Joseph A. O'Sullivan, Erik J. Sirevaag, and John W. Rohrbaugh. 2012. ECG Biometric Recognition: A Comparative Analysis. *IEEE Transactions on Information Forensics and Security* 7, 6 (dec 2012), 1812–1824. https://doi.org/10.1109/tifs.2012.2215324

[146] Yoshitaka Ohshio, Haruka Adachi, Kenta Iwai, Takanobu Nishiura, and Yoichi Yamashita. 2018. Active Speech Obscuration with Speaker-dependent Human Speech-like Noise for Speech Privacy. In *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*. IEEE, 1252–1255. https://doi.org/10.23919/apsipa.2018.8659754

[147] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q.-I. Moro. 2003. MCYT baseline corpus: a bimodal biometric database. *IEE Proceedings - Vision, Image, and Signal Processing* 150, 6 (2003), 395. https://doi.org/10.1049/ip-vis:20031078

[148] Vassil Panayotov, Guoguo Chen, Daniel Povey, and Sanjeev Khudanpur. 2015. Librispeech: An ASR corpus based on public domain audio books. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 5206–5210. https://doi.org/10.1109/icassp.2015.7178964

[149] Julien Pansiot, Danail Stoyanov, Douglas McIlwraith, Benny P.L. Lo, and G. Z. Yang. 2007. Ambient and Wearable Sensor Fusion for Activity Recognition in Healthcare Monitoring Systems. In *4th International Workshop on Wearable and Implantable Body Sensor Networks (BSN 2007)*. Springer, Springer Berlin Heidelberg, 208–212. https://doi.org/10.1007/978-3-540-70994-7_36

[150] Sree Hari Krishnan Parthasarathi, Herve Bourlard, and Daniel Gatica-Perez. 2011. LP Residual Features for Robust, Privacy-Sensitive Speaker Diarization. In *Interspeech*.

[151] Sree Hari Krishnan Parthasarathi, H. Bourlard, and D. Gatica-Perez. 2013. Wordless Sounds: Robust Speaker Diarization Using Privacy-Preserving Audio Representations. *IEEE Transactions on Audio, Speech, and Language Processing* 21, 1 (jan 2013), 85–98. https://doi.org/10.1109/tasl.2012.2215588

[152] Sree Hari Krishnan Parthasarathi, Mathew Magimai.-Doss, Daniel Gatica-Perez, and Hervé Bourlard. 2009. Speaker change detection with privacy-preserving audio cues. In *Proceedings of the 2009 international conference on Multimodal interfaces - ICMI-MLMI '09*. ACM Press, 343. https://doi.org/10.1145/1647314.1647385

[153] Manas A. Pathak and Bhiksha Raj. 2012. Privacy-preserving speaker verification as password matching. In *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 1849–1852. https://doi.org/10.1109/icassp.2012.6288262

[154] David I. Perrett, Sean N. Talamas, Patrick Cairns, and Audrey J. Henderson. 2020. Skin Color Cues to Human Health: Carotenoids, Aerobic Fitness, and Body Fat. *Frontiers in Psychology* 11 (mar 2020). https://doi.org/10.3389/fpsyg.2020.00392

[155] Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 1–12. https://doi.org/10.1145/3290605.3300340

[156] R. Plamondon and S.N. Srihari. 2000. Online and off-line handwriting recognition: a comprehensive survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 22, 1 (2000), 63–84. https://doi.org/10.1109/34.824821

[157] Kurt Plarre, Andrew Raij, Syed Monowar Hossain, Amin Ahsan Ali, Motohiro Nakajima, Mustafa Al'absi, Emre Ertin, Thomas Kamarck, Santosh Kumar, Marcia Scott, Daniel Siewiorek, Asim Smailagic, and Lorentz E. Wittmers. 2011. Continuous inference of psychological stress from sensory measurements collected in the natural environment. In *Proceedings of the 10th ACM/IEEE International Conference on Information Processing in Sensor Networks*. 97–108.

[158] M. Pobar and I. Ipsic. 2014. Online speaker de-identification using voice transformation. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 1264–1267. https://doi.org/10.1109/mipro.2014.6859761

[159] Bogdan Pogorelc, Zoran Bosnić, and Matjaž Gams. 2011. Automatic recognition of gait-related health problems in the elderly using machine learning. *Multimedia Tools and Applications* 58, 2 (nov 2011), 333–354. https://doi.org/10.1007/s11042-011-0786-1

[160] Frank E. Pollick, Jim W. Kay, Katrin Heim, and Rebecca Stringer. 2005. Gender recognition from point-light walkers. *Journal of Experimental Psychology: Human Perception and Performance* 31, 6 (dec 2005), 1247–1265. https://doi.org/10.1037/0096-1523.31.6.1247

[161] Alex Poole and Linden J. Ball. 2006. Eye Tracking in HCI and Usability Research. In *Encyclopedia of Human Computer Interaction*. IGI Global, 211–219. https://doi.org/10.4018/978-1-59140-562-7.ch034

[162] Jose Portelo, Alberto Abad, Bhiksha Raj, and Isabel Trancoso. 2013. Secure Binary Embeddings of Front-End Factor Analysis for Privacy Preserving Speaker Verification. (2013), 2494–2498.

[163] Jose Portelo, Bhiksha Raj, Alberto Abad, and Isabel Trancoso. 2014. Privacy-preserving speaker verification using secure binary embeddings. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 1268–1272. https://doi.org/10.1109/mipro.2014.6859762

[164] Jiří Přibil, Anna Přibilová, and Jindřich Matoušek. 2018. Evaluation of speaker de-identification based on voice gender and age conversion. *Journal of Electrical Engineering* 69, 2 (mar 2018), 138–147. https://doi.org/10.2478/jee-2018-0017

[165] Jianwei Qian, Haohua Du, Jiahui Hou, Linlin Chen, Taeho Jung, and Xiangyang Li. 2021. Speech Sanitizer: Speech Content Desensitization and Voice Anonymization. *IEEE Transactions on Dependable and Secure Computing* (2021), 1–1. https://doi.org/10.1109/tdsc.2019.2960239

[166] Jianwei Qian, Haohua Du, Jiahui Hou, Linlin Chen, Taeho Jung, and Xiang-Yang Li. 2018. Hidebehind: Enjoy Voice Input with Voiceprint Unclonability and Anonymity. In *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*. ACM, 82–94. https://doi.org/10.1145/3274783.3274855

[167] Jianwei Qian, Feng Han, Jiahui Hou, Chunhong Zhang, Yu Wang, and Xiang-Yang Li. 2018. Towards Privacy-Preserving Speech Data Publishing. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. IEEE, 1079–1087. https://doi.org/10.1109/infocom.2018.8486250

[168] Yaron Rachlin and Dror Baron. 2008. The secrecy of compressed sensing measurements. In *2008 46th Annual Allerton Conference on Communication, Control, and Computing*. IEEE, 813–817. https://doi.org/10.1109/allerton.2008.4797641

[169] Vibhor Rastogi and Suman Nath. 2010. Differentially private aggregation of distributed time-series with transformation and encryption. In *Proceedings of the 2010 ACM SIGMOD International Conference on Management of data*. ACM, 735–746. https://doi.org/10.1145/1807167.1807247

[170] SRS Reddy, Sravani Nalluri, Subramanyam Kunisetti, S Ashok, and B Venkatesh. 2019. Content-based movie recommendation system using genre correlation. In *Smart Intelligent Computing and Applications*. Springer, 391–397.

[171] Douglas A. Reynolds. 1995. Speaker identification and verification using Gaussian mixture speaker models. *Speech Communication* 17, 1 (aug 1995), 91–108. https://doi.org/10.1016/0167-6393(95)00009-d

[172] Douglas A. Reynolds, Thomas F. Quatieri, and Robert B. Dunn. 2000. Speaker Verification Using Adapted Gaussian Mixture Models. *Digital Signal Processing* 10, 1 (jan 2000), 19–41. https://doi.org/10.1006/dspr.1999.0361

[173] Slobodan Ribaric, Aladdin Ariyaeeinia, and Nikola Pavesic. 2016. De-identification for privacy protection in multimedia content: A survey. *Signal Processing: Image Communication* 47 (sep 2016), 131–151. https://doi.org/10.1016/j.image.2016.05.020

[174] Napa Sae-Bae and Nasir Memon. 2013. A Simple and Effective Method for Online Signature Verification. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, 1–12.

[175] Napa Sae-Bae, Nasir Memon, Katherine Isbister, and Kowsar Ahmed. 2014. Multitouch Gesture-Based Authentication. *IEEE Transactions on Information Forensics and Security* 9, 4 (apr 2014), 568–582. https://doi.org/10.1109/tifs.2014.2302582

[176] Nazir Saleheen, Supriyo Chakraborty, Nasir Ali, Md Mahbubur Rahman, Syed Monowar Hossain, Rummana Bari, Eugene Buder, Mani Srivastava, and Santosh Kumar. 2016. MSieve: Differential Behavioral Privacy in Time Series of Mobile Sensor Data. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '16)*. ACM, New York, NY, USA, 706–717. https://doi.org/10.1145/2971648.2971753

[177] Michael Sherman, Gradeigh Clark, Yulong Yang, Shridatt Sugrim, Arttu Modig, Janne Lindqvist, Antti Oulasvirta, and Teemu Roos. 2014. User-generated free-form gestures for authentication. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services (MobiSys '14)*. ACM, New York, NY, USA, 176–189. https://doi.org/10.1145/2594368.2594375

[178] Yogendra Narain Singh and Phalguni Gupta. 2008. ECG to Individual Identification. In *2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems*. IEEE, 1–8. https://doi.org/10.1109/btas.2008.4699343

[179] David Snyder, Daniel Garcia-Romero, Gregory Sell, Daniel Povey, and Sanjeev Khudanpur. 2018. X-Vectors: Robust DNN Embeddings for Speaker Recognition. In *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 5329–5333. https://doi.org/10.1109/icassp.2018.8461375

[180] Petr Sojka, Aleš Horák, Ivan Kopeček, and Karel Pala (Eds.). 2014. *Text, Speech and Dialogue: 17th International Conference, TSD 2014, Brno, Czech Republic, September 8-12, 2014. Proceedings*. Lecture Notes in Computer Science, Vol. 8655. Springer International Publishing. https://doi.org/10.1007/978-3-319-10816-2

[181] Brij Mohan Lal Srivastava, Nathalie Vauquier, Md Sahidullah, Aurelien Bellet, Marc Tommasi, and Emmanuel Vincent. 2020. Evaluating Voice Conversion-based Privacy Protection against Informed Attackers. (may 2020). https://doi.org/10.1109/icassp40776.2020.9053868

[182] Julian Steil, Inken Hagestedt, Michael Xuelin Huang, and Andreas Bulling. 2019. Privacy-Aware Eye Tracking Using Differential Privacy. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications (ETRA '19)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3314111.3319915

[183] Tino Stöckel, Robert Jacksteit, Martin Behrens, Ralf Skripitz, Rainer Bader, and Anett Mau-Moeller. 2015. The mental representation of the human gait in young and older adults. *Frontiers in Psychology* 6 (2015), 943. https://doi.org/10.3389/fpsyg.2015.00943

[184] Fahim Sufi, Seedahmed Mahmoud, and Ibrahim Khalil. 2008. A new ECG obfuscation method: A joint feature extraction & corruption approach. In *2008 International Conference on Information Technology and Applications in Biomedicine*. IEEE, 334–337. https://doi.org/10.1109/itab.2008.4570644

[185] Fahim Sufi, Seedahmed Mahmoud, and Ibrahim Khalil. 2008. A wavelet based secured ECG distribution technique for patient centric cpproach. In *2008 5th International Summer School and Symposium on Medical Devices and Biosensors*. IEEE, 301–304. https://doi.org/10.1109/issmdbs.2008.4575079

[186] Shravani Sur and VK Sinha. 2009. Event-related potential: An overview. *Industrial Psychiatry Journal* 18, 1 (2009), 70. https://doi.org/10.4103/0972-6748.57865

[187] Takahiro Tamesue and Tetsuro Saeki. 2014. Sound masking for achieving speech privacy with parametric acoustic array speaker. In *2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS)*. IEEE, 1134–1137. https://doi.org/10.1109/scis-isis.2014.7044805

[188] Pin Shen Teh, Andrew Beng Jin Teoh, and Shigang Yue. 2013. A Survey of Keystroke Dynamics Biometrics. *The Scientific World Journal* 2013 (2013), 1–24. https://doi.org/10.1155/2013/408280

[189] Pin Shen Teh, Ning Zhang, Andrew Beng Jin Teoh, and Ke Chen. 2016. A survey on touch dynamics authentication in mobile devices. *Computers & Security* 59 (jun 2016), 210–235. https://doi.org/10.1016/j.cose.2016.03.003

[190] Jing Tian, Chengzhang Qu, Wenyuan Xu, and Song Wang. 2013. KinWrite: Handwriting-Based Authentication Using Kinect. 93 (2013), 94.

[191] Ngoc-Dung T. Tieu, Huy H. Nguyen, Fuming Fang, Junichi Yamagishi, and Isao Echizen. 2019. An RGB Gait Anonymization Model for Low-Quality Silhouettes. In *2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*. IEEE, 1686–1693. https://doi.org/10.1109/apsipaasc47483.2019.9023188

[192] Ngoc-Dung T. Tieu, Huy H. Nguyen, Hoang-Quoc Nguyen-Son, Junichi Yamagishi, and Isao Echizen. 2017. An approach for gait anonymization using deep learning. In *2017 IEEE Workshop on Information Forensics and Security (WIFS)*. IEEE, 1–6. https://doi.org/10.1109/wifs.2017.8267657

[193] Ngoc-Dung T. Tieu, Huy H. Nguyen, Hoang-Quoc Nguyen-Son, Junichi Yamagishi, and Isao Echizen. 2019. Spatio-temporal generative adversarial network for gait anonymization. *Journal of Information Security and Applications* 46 (jun 2019), 307–319. https://doi.org/10.1016/j.jisa.2019.03.002

[194] Quang Nhat Tran, Benjamin P. Turnbull, and Jiankun Hu. 2021. Biometrics and Privacy-Preservation: How Do They Evolve? *IEEE Open Journal of the Computer Society* 2 (2021), 179–191. https://doi.org/10.1109/ojcs.2021.3068385

[195] Nikolaus F. Troje. 2002. Decomposing biological motion: A framework for analysis and synthesis of human gait patterns. *Journal of Vision* 2, 5 (sep 2002), 2. https://doi.org/10.1167/2.5.2

[196] TypingDNA. [n.d.]. Webpage. https://www.typingdna.com Accessed: 01.06.2019.

[197] Tavish Vaidya and Micah Sherr. 2019. You Talk Too Much: Limiting Privacy Exposure Via Voice Input. In *2019 IEEE Security and Privacy Workshops (SPW)*. IEEE, 84–91. https://doi.org/10.1109/spw.2019.00026

[198] Gabriele Vassallo, Tim Van hamme, Davy Preuveneers, and Wouter Joosen. 2017. Privacy-Preserving Behavioral Authentication on Smartphones. In *Proceedings of the First International Workshop on Human-centered Sensing, Networking, and Systems*. ACM, 1–6. https://doi.org/10.1145/3144730.3144731

[199] Voice Vault. [n.d.]. VoiceVault Voice Biometric Authentication. Webpage. https://voicevault.com/ Accessed: 01.06.2019.

[200] Changsheng Wan, Li Wang, and Vir V. Phoha. 2019. A Survey on Gait Recognition. *Comput. Surveys* 51, 5 (jan 2019), 1–35. https://doi.org/10.1145/3230633

[201] Shuo Wang, Ming Jiang, Xavier Morin Duchesne, Elizabeth A. Laugeson, Daniel P. Kennedy, Ralph Adolphs, and Qi Zhao. 2015. Atypical Visual Saliency in Autism Spectrum Disorder Quantified through Model-Based Eye Tracking. *Neuron* 88, 3 (nov 2015), 604–616. https://doi.org/10.1016/j.neuron.2015.09.042

[202] Leon Willenborg and Ton de Waal. 2001. *Elements of Statistical Disclosure Control*. Springer New York, New York. https://doi.org/10.1007/978-1-4613-0121-9

[203] Shun-Chi Wu, Peng-Tzu Chen, A. Lee Swindlehurst, and Pei-Lun Hung. 2019. Cancelable Biometric Recognition With ECGs: Subspace-Based Approaches. *IEEE Transactions on Information Forensics and Security* 14, 5 (may 2019), 1323–1336. https://doi.org/10.1109/tifs.2018.2876838

[204] Danny Wyatt, Tanzeem Choudhury, and Jeff Bilmes. 2007. Conversation Detection and Speaker Segmentation in Privacy-Sensitive Situated Speech Data. In *Eighth Annual Conference of the International Speech Communication Association*.

[205] Sherif Yacoub, Steve Simske, Xiaofan Lin, and John Burns. 2003. Recognition of emotions in interactive voice response systems. In *Eighth European conference on speech communication and technology*.

[206] Roman V. Yampolskiy and Venu Govindaraju. 2010. Taxonomy of Behavioural Biometrics. In *Behavioral Biometrics for Human Identification*. IGI Global, 1–43. https://doi.org/10.4018/978-1-60566-725-6.ch001

[207] Qing Yang, Tao Wang, Ning Su, Shifu Xiao, and Zoi Kapoula. 2012. Specific saccade deficits in patients with Alzheimer's disease at mild to moderate stage and in patients with amnestic mild cognitive impairment. *AGE* 35, 4 (may 2012), 1287–1298. https://doi.org/10.1007/s11357-012-9420-z

[208] Yue Yao, Josephine Plested, Tom Gedeon, Yuchi Liu, and Zhengjie Wang. 2019. Improved Techniques for Building EEG Feature Filters. In *2019 International Joint Conference on Neural Networks (IJCNN)*. IEEE, IEEE, 1–6. https://doi.org/10.1109/ijcnn.2019.8852302

[209] Mang Ye, Jianbing Shen, Gaojie Lin, Tao Xiang, Ling Shao, and Steven C.H. Hoi. 2021. Deep Learning for Person Re-identification: A Survey and Outlook. *IEEE Transactions on Pattern Analysis and Machine Intelligence* (2021), 1–1. https://doi.org/10.1109/tpami.2021.3054775

[210] Dit-Yan Yeung, Hong Chang, Yimin Xiong, Susan George, Ramanujan Kashi, Takashi Matsumoto, and Gerhard Rigoll. 2004. SVC2004: First International Signature Verification Competition. In *Biometric Authentication*, David Zhang and Anil K. Jain (Eds.). Vol. 3072. Springer Berlin Heidelberg, 16–22. https://doi.org/10.1007/978-3-540-25948-0_3 Series Title: Lecture Notes in Computer Science.

[211] Galit Yovel and Alice J. O'Toole. 2016. Recognizing People in Motion. *Trends in Cognitive Sciences* 20, 5 (may 2016), 383–395. https://doi.org/10.1016/j.tics.2016.02.005

[212] Emna Kalai Zaghouani, Adel Benzina, and Rabah Attia. 2017. ECG based authentication for e-healthcare systems: Towards a secured ECG features transmission. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 1777–1783. https://doi.org/10.1109/iwcmc.2017.7986553

[213] Emna Kalai Zaghouani, Adel Benzina, and Rabah Attia. 2017. ECG biometrie template protection based on secure sketch scheme. In *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, 1–5. https://doi.org/10.23919/softcom.2017.8115526

[214] Mohammad-Reza Zare-Mirakabad, Fatemeh Kaveh-Yazdy, and Mohammad Tahmasebi. 2013. Privacy preservation by k-anonymizing Ngrams of time series. In *2013 10th International ISC Conference on Information Security and Cryptology (ISCISC)*. 1–6. https://doi.org/10.1109/ISCISC.2013.6767335

[215] Guanglin Zhang, Sifan Ni, and Ping Zhao. 2020. Enhancing Privacy Preservation in Speech Data Publishing. *IEEE Internet of Things Journal* 7, 8 (aug 2020), 7357–7367. https://doi.org/10.1109/jiot.2020.2983228

[216] Ni Zhang and Yoshinori Yaginuma. 2012. A privacy-preserving and language-independent speaking detecting and speaker diarization approach for spontaneous conversation using microphones. In *2012 IEEE 11th International Conference on Signal Processing*. IEEE, 499–502. https://doi.org/10.1109/icosp.2012.6491534

[217] Jianwei Zheng, Jianming Zhang, Sidy Danioko, Hai Yao, Hangyuan Guo, and Cyril Rakovski. 2020. A 12-lead electrocardiogram database for arrhythmia research covering more than 10,000 patients. *Scientific Data* 7, 1 (feb 2020). https://doi.org/10.1038/s41597-020-0386-x

[218] Nan Zheng, Aaron Paloski, and Haining Wang. 2016. An Efficient User Verification System Using Angle-Based Mouse Movement Biometrics. *ACM Transactions on Information and System Security* 18, 3 (apr 2016), 1–27. https://doi.org/10.1145/2893185

[219] Shuxin Zheng, Qi Meng, Taifeng Wang, Wei Chen, Nenghai Yu, Zhi-Ming Ma, and Tie-Yan Liu. 2017. Asynchronous Stochastic Gradient Descent with Delay Compensation. In *Proceedings of the 34th International Conference on Machine Learning - Volume 70* (Sydney, NSW, Australia) *(ICML'17)*. JMLR.org, 4120–4129. https://doi.org/10.5555/3305890.3306107

[220] Shuai Zheng, Junge Zhang, Kaiqi Huang, Ran He, and Tieniu Tan. 2011. Robust view transformation model for gait recognition. In *2011 18th IEEE International Conference on Image Processing*. IEEE, 2073–2076. https://doi.org/10.1109/icip.2011.6115889

[221] Yu Zhong and Yunbin Deng. 2015. A Survey on Keystroke Dynamics Biometrics: Approaches, Advances, and Evaluations. In *Gate to Computer Science and Research*. Number 1. Science Gate Publishing P.C., 1–22. https://doi.org/10.15579/gcsr.vol2.ch1

[222] Mohammad Zohaib. 2018. Dynamic Difficulty Adjustment (DDA) in Computer Games: A Review. *Advances in Human-Computer Interaction* 2018 (nov 2018), 1–12. https://doi.org/10.1155/2018/5681652