Engineering Standards and Ethics in Automated Biometrics

by

Grant P. Kirby

A thesis submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Master of Science

Auburn, Alabama
May 1, 2021

Keywords: biometrics, authentication, multimodal, irrevocable, cancelable

Approved by

John Y. Hung, Chair, Professor of Electrical and Computer Engineering
Thaddeus A. Roppel, Associate Professor of Electrical and Computer Engineering
Jason V. Clark, Assistant Professor of Electrical and Computer Engineering

Abstract

This work explores a two-part question: (1) what are the most recent engineering standards that govern AI development and implementation in the field of biometrics and (2) what ethical implications do they have for society? For the sake of brevity, the application area is focused on biometrics, but the research methods and conclusions may have broader applicability and implications.

Acknowledgments

I would like to thank the Auburn professors and staff as well as the members of my committee that have helped me immensely on this journey. Their guidance and encouragement have been refreshing and enlightening. I would also like to thank my parents, Howell and Coby Kirby, for their unfailing support in my pursuit of this degree. Lastly, I would like to thank my wife Annie Kirby for her encouragement in this endeavor. She has been so understanding during this entire process and I truly would not have been able to complete the task were it not for her.

Table of Contents

List of Figures

List of Abbreviations

A/IS	Autonomous/Intelligent Systems
AI	Artificial Intelligence
BIPA	Biometric Information Privacy Act
BOPS	Biometric Open Protocol Standard
CBP	Customs and Border Patrol
CDT	Center for Democracy and Technology
CFRPA	Commercial Facial Recognition Privacy Act
DET	Detection Error Tradeoff
DHS	Department of Homeland Security
DPIAC	Data Privacy and Integrity Advisory Council
EER	Equal Error Rate
FAA	Federal Aviation Administration
FAR	False Acceptance Rate
FIPS	Federal Information Processing Standards
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Rejection Rate
FTA	Failure to Acquire
GDPR	General Data Protection Regulation
ICAO	International Civil Aviation Organization

IEC	International Electrotechnical Commission
ISO	International Organization of Standardization
JTC	Joint Technical Committee
LOS	Line of Sight
MRTD	Machine Readable Travel Document
NLOS	Non-Line of Sight
PII	Personally Identifying Information
PIV	Personal Identity Verification
ROC	Receiver Operating Characteristic
TAR	True Acceptance Rate
ZEMFA	Zero-Effort Multi-Factor Authentication

Vita

Grant Patrick Kirby was born August 13th 1981 to William Howell Kirby and Eleanor Coborn Kirby in Birmingham Alabama. He graduated from Parkview High School, located in Lilburn Georgia in 2000. He received a B.A. in Philosophy, graduating magna cum laude from the University of Georgia in Athens, GA in 2005. He is employed by Auburn Utilities & Energy Department, where he utilizes energy data analysis tools and skills to create a more efficient energy system. He is also pursuing a masters' degree in the Department of Electrical and Computer Engineering, with his most recent research activities in the fields of biometrics and robotics.

I. BACKGROUND

Considered by some to be the fourth industrial revolution, artificial intelligence (AI) is now poised to upend nearly every aspect of modern life. Increases in autonomous/intelligent systems (A/IS) are giving rise to technologies in which humans are—more and more—relinquishing any meaningful authority over the systems that affect them. This is, in fact, the stated engineering goal of some A/IS systems: to eliminate the potentially erroneous human element. One developing area of AI research that may steadily eliminate the possibility of human error is the field of biometrics—the study of unique quantifiable human characteristics and features for the purposes of classification, identification, and authentication.

1.1 An Emerging Engineering Field

As the world approaches an increasingly algorithmic future, various players are expressing their concern about both the potential benefits and dangers of artificially intelligent agents. Of particular interest is the field of biometrics. Many companies and government bodies have already proposed their own standards and benchmarks regarding biometric privacy and safety protocols. These regulatory standards, however, are largely nascent and lag fast-paced technological development. Large-scale consensus as well as significant legal and legislative issues also exist. In addition, the impact on human well-being and the accompanying ethical effects of those technologies have been poorly examined in the literature. According to the most recent *IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being,* 'there is no widely accepted set of recommendations, standards, best practices, guidelines, or regulations for contributing to or helping safeguard or improve human well-being…A/IS technologies are relatively novel and their use and the understanding of intended and

unintended impacts are hard to predict. A/IS impact human well-being in many complex ways, some known and some unknown' [1].

A/IS biometric technology appears to be achieving steady progress, but with some setbacks. Similarly, technological revolutions of the past have tended to undergo an initial period of upheaval as they struggle to find a firm footing. The early electrification of the United States, for instance, was largely an experimental endeavor with competing business and governmental interests seeking to gain a foothold. It was not until shared engineering standards and electrical codes were adopted that the instability largely subsided, and progress accelerated rapidly. The same was true of wireless communication technology. A/IS biometric research is now experiencing many of the same founding struggles as those groundbreaking technologies of the past. The rules are currently being written and rewritten over again on a constant basis.

1.2 Standardization and Regulatory Environment

At present, many normative documents are helping to protect and stabilize the industry as well as foster its rapid innovation. Standards such as the *IEEE Std 2410-2019 Biometric Open Protocol Standard (BOPS)* establishes as its purpose to 'provide a biometric-agnostic security protocol for authentication, identification, and liveness' [2]. Other governing documents addressed in the standard regarding Personally Identifying Information (PII) will be discussed in later sections. As the need for safeguarding PII remains important, governing standards for authentication and identification continue to develop and guide the process.

AI/S biometrics are a recent development. Many security loopholes and vulnerabilities that were previously exploited have been shored up as our understanding of the problem has increased. However, the situation continues to evolve quickly, and as mentioned at the beginning, a keen awareness and planning for many legitimate ethical and security concerns is lagging.

The United States, it seems, has no comprehensive federal law in place pertaining to biometric data privacy. The European Union (EU), however, issued its standard for biometric data protection in the form of the General Data Protection Regulation (GDPR), effective May 2018 [3]. The GDPR governs the handling of member states consumer data and seeks to harmonize its own disparate assortment of privacy laws. GDPR has had an effect in the United States as many international organizations have had to modify their business practices to become compliant. The most recent proposed U.S. federal legislation, the Commercial Facial Recognition Privacy Act (CFRPA), would become the first federal biometrics legislation if it were to pass into law [4].

At the state level, biometric privacy laws are a patchwork of individual standards and regulations. Notably, Illinois is the strongest in this regard. The Biometric Information Privacy Act (BIPA) was passed by the Illinois General Assembly in 2008 [5]. Since its inception, several class-action lawsuits have been brought against employers and other institutions for alleged BIPA violations. Many states, however, have no such laws or even basic standards in place regarding biometric privacy, data maintenance and security, the legal/ethical impact of biometric intrusion, etc. Of the standards that do exist regarding biometrics, many of them are based around the notion of voluntary compliance. Unlike other government regulatory agencies such as the Federal Aviation Administration (FAA) or the Environmental Protection Agency (EPA), AI and advanced biometric technology has no authoritative agency to regulate and monitor its growth in the United States.

Unchecked AI technology has drawn criticism and attention from various advocacy groups. The Center for Democracy and Technology (CDT), a non-profit advocacy group, offered a clear rebuke in 2019 in response to a call for public comment by the Department of Homeland Security (DHS). The draft report titled *Privacy Recommendations in Connection with the Use of Facial*

Recognition Technology was formulated by the Data Privacy and Integrity Advisory Council (DPIAC) [6]. In its response to DPIAC, CDT notes that Customs and Border Patrol (CBP) is currently using facial recognition technology against U.S. citizens despite not having Congressional approval [7]. Moreover, CDT's document highlights other large-scale problems that have failed to be addressed including the tendency toward mission creep and the issues surrounding algorithmic discrimination and inaccuracy. It is clear that whatever may be understood technically about automated biometrics, the justification, codification, and legislation of its applicable use in society is still very much an open question.

1.3 Industry Outlook and Public Acceptance

The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update outlines ten overarching strategies for maintaining America's leadership in AI [8]. Among these are the importance of continued innovation, research and development, sustained funding and partnership between public and private institutions, a focus on human-AI collaboration, the availability of public training datasets, as well as the growing public concern about the potential for abuse, etc. Many guidelines and recommendations are proposed in the document. But the developing standards are difficult to enforce.

Unlike more established industry sectors, biometrics has yet to garner a widely accepted trustworthiness among members of the public. There is still significant social distrust of the technology among various populations. This attitude is likely changing, however, as more and more individuals enjoy the power and convenience of biometric technology in countless ways: cell phones, computers, cars, access control systems, banks, health service kiosks, airports, border crossings, government centers, libraries, community centers, etc. The force of law and the threat of enforceable punishment for biometric violations in the United States has yet to become

standardized or codified, likely because the technology is still emergent, but also because the technology itself and the prevailing issues are poorly understood.

1.4 Overview

The review in the previous sections demonstrate that the engineering field of biometrics is in the early stages of its evolution. Although highly developed in many respects, automated biometrics still suffers from significant technological and social dilemmas that are likely to remain entrenched if the field is not further standardized and cooperatively legislated at a global level. As public resistance to biometrics begins to wane and the field begins to embed into societal infrastructure, fresh new problems will arise in both technological and ethical contexts. The remainder of this work is organized as follows. Chapter II examines the standards and metrics that have evolved for biometric technology. Chapter III highlights the leading-edge field of distanced biometrics and how those fields differ in outlook and approach. Chapter IV examines current technical and social problems for the field of biometrics. Chapter V discusses some of the ethical issues surrounding biometrics such as privacy and irrevocability in society. Chapter VI provides some concluding remarks about the current and future state of biometric standards and ethics as well as important future work for the field.

II. BIOMETRIC STANDARDIZATION

2.1 Biometric Standards

Biometric testing standards and verification benchmarks have been established internationally across most continents for both industry and government. In 2002, a Joint Technical Committee (JTC) was formed between the International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC) to establish generic human biometric standards [9]. *JTC SC37 Biometrics*, focused broadly on grappling with pressing biometric issues such as interoperability, data interchange formats, biometric profiles, evaluation criteria, methodologies for performance testing, and societal aspects. Formal liaisons such as the International Civil Aviation Organization (ICAO) were consulted for their work in Machine Readable Travel Documents (MRTD's) as well as other financial services and IT related committees. The global standard *ISO/IEC 19795-1: 2006 Information Technology—Biometric performance testing and reporting* remains one of the broadest governing documents in the field. It establishes standardized and unambiguous protocols for evaluating various biometric screening techniques including fingerprint, iris, and facial recognition systems. These standardized metrics are based on empirical estimates of probability.

2.2 Relevant Terms

To understand the underlying broader issues facing this engineering field, it is important to have a thorough knowledge of the terms and evaluation criteria for biometric systems. For verification, the metrics from [10] are:

False Match Rate (FMR):

An empirical estimate of the probability (the percentage of attempts) at which the system incorrectly declares that a biometric sample belongs to the claimed identity when the sample actually belongs to a different subject (impostor).

False Non-Match Rate (FNMR):

An empirical estimate of the probability (the percentage of attempts) at which the system incorrectly rejects a claimed identity when the sample actually belongs to the subject (genuine user).

Failure to Acquire Rate (FTA):

The proportion of attempts for which the system fails to produce a sample of sufficient quality.

False Acceptance Rate (FAR) and False Rejection Rate (FRR):

FAR/FRR are often used interchangeably in the literature in place of FMR/FNMR but are subtly different, which can be confusing. FMR and FNMR are measurement errors that occur at the level of the algorithm. The biometric sample either matched or did not match a stored template in the database falsely. FAR and FRR are system-level errors that may include multiple failed verification attempts (i.e. Failure to Acquire) that affect the final accept or reject decision.

$$\mathbf{FAR = FMR * (1 – FTA)}$$

$$\mathbf{FRR = FNMR * (1\text{-}FTA)}$$

True Acceptance Rate (TAR):

It is defined as: $\mathbf{TAR = 1\text{-}FRR}$

Equal Error Rate (EER):

The EER is the operating threshold at which FAR is equal to FRR. The EER is used in biometrics to measure system performance. In general, the lower the EER, the higher the accuracy of the biometric system.

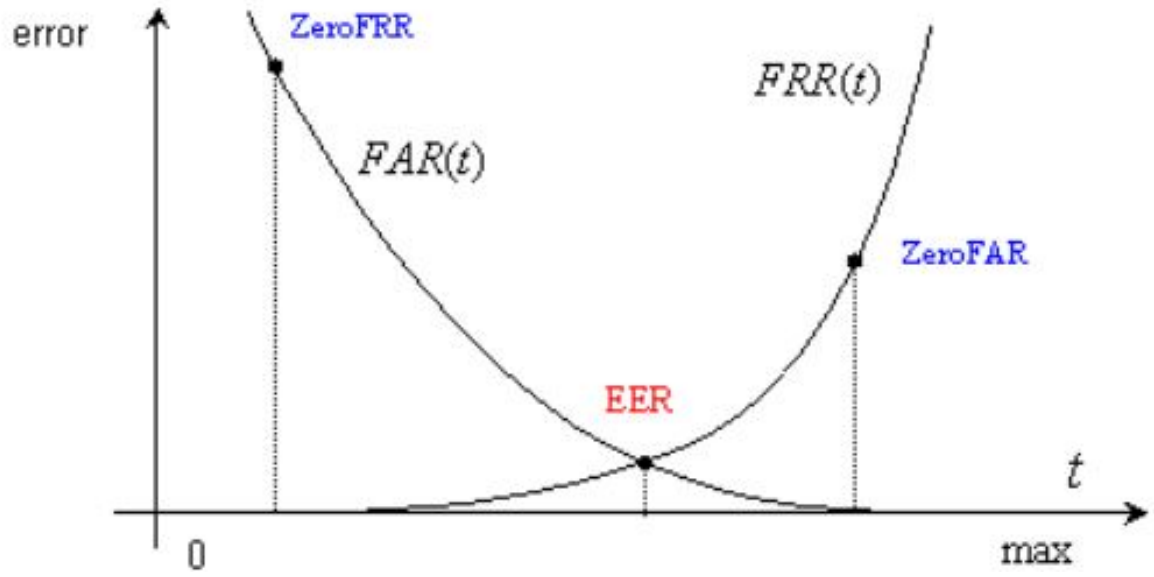

Figure 2.1: Equal Error Rate [11]

Receiver Operating Characteristic (ROC):

A ROC curve plots the TAR (1-FRR) in the Y-axis versus FAR in the X-axis. It is one way to visualize the accuracy of a biometric algorithm. The point at the top left-hand corner of the graph represents perfect accuracy. Thus, the biometric algorithm whose ROC curve is closest to this point is the most accurate.

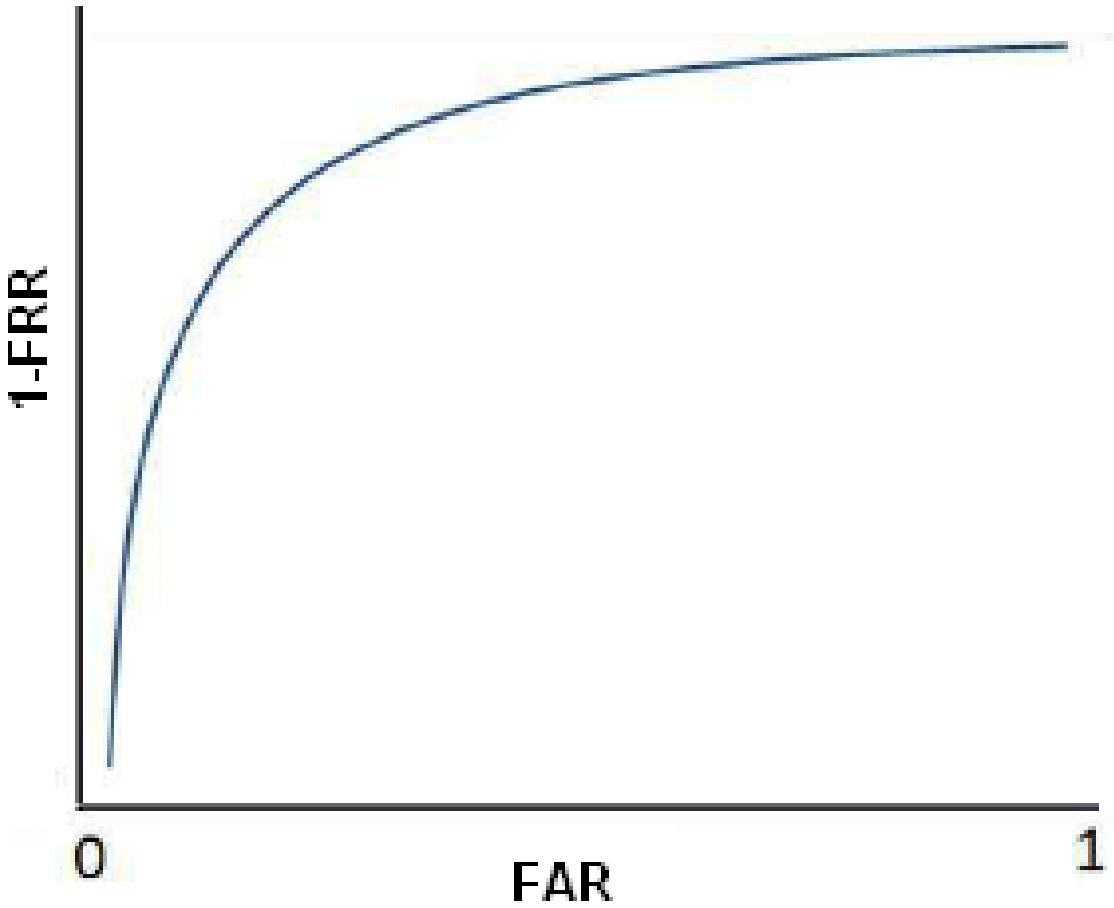

Figure 2.2: Receiver Operating Characteristic Curve [12]

Detection Error Tradeoff (DET):

A DET curve is similar to the ROC curve except that the axes are often scaled non-linearly to highlight the critical operating region. A unity slope line extending from the origin will intersect the DET curve at the EER.

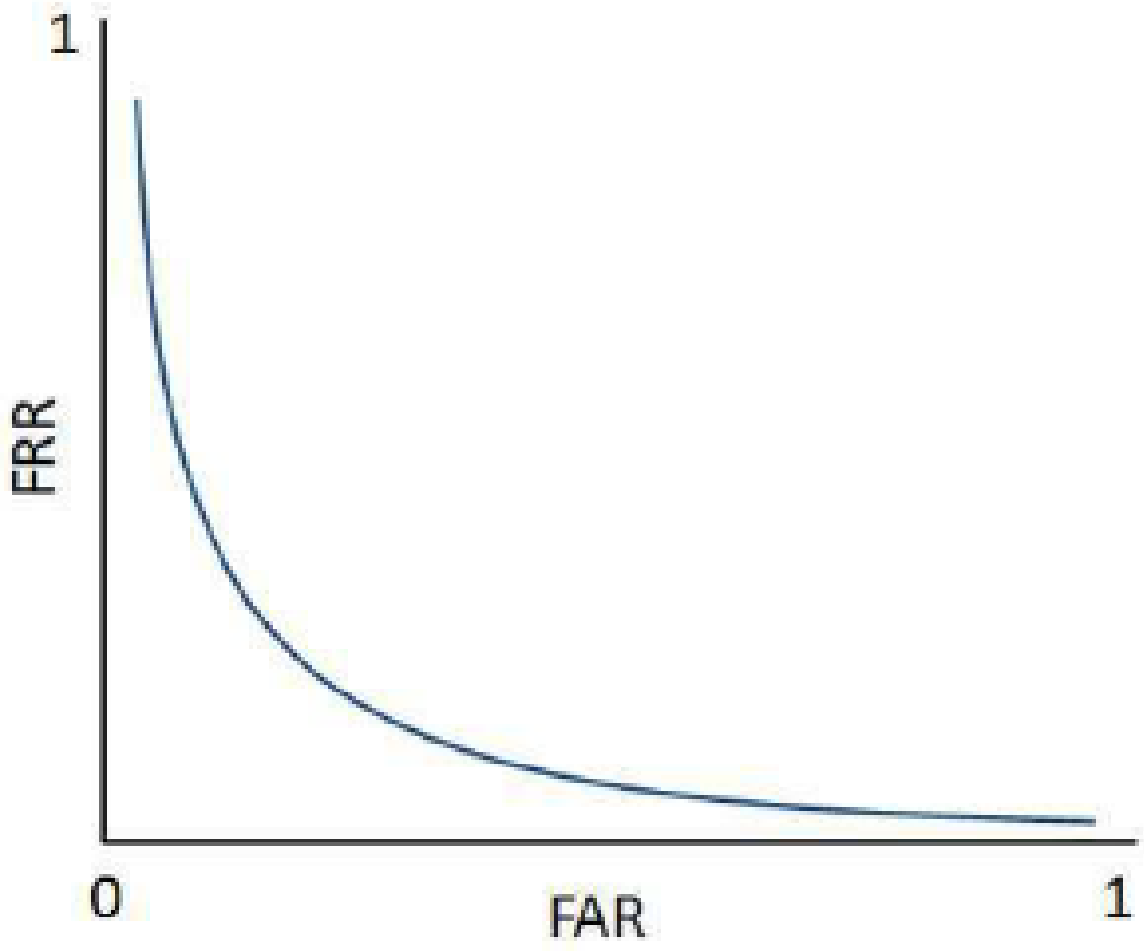

Figure 2.3: Detection Error Tradeoff Curve [13]

All automated biometric systems function in a similar fashion as illustrated in Figure 2.4. The process begins with the enrollment phase. During this phase, a biometric sample—fingerprint, facial scan, iris, etc.—is presented to the sensor for capture. If the sample is of sufficient quality, then a template is generated and stored in the enrollment database. If the sample is not of sufficient quality, then a recapture attempt is initiated, and the process repeats until sufficient quality is reached. A recapture is also known as a Failure to Acquire (FTA) when calculating biometric system metrics. Sufficient quality is defined based on certain signal processing characteristics: proper segmentation, proper feature extraction, etc. (See [19] in Additional References for more detailed information).

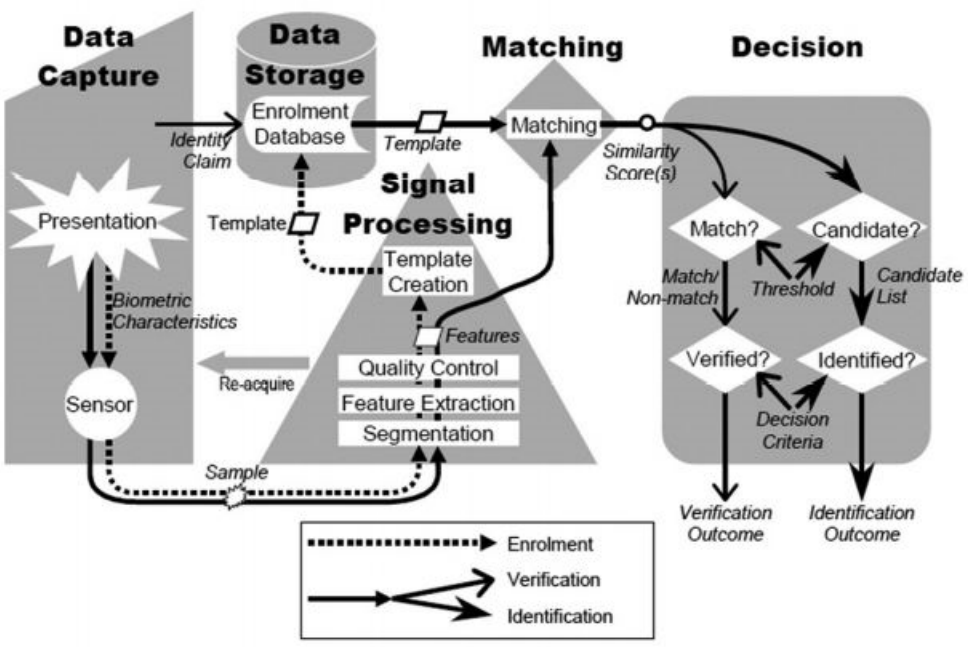

Figure 2.4: Automated Biometric System Process [14]

Once a template is generated and stored, it can be compared and matched with any future samples collected. This is referred to as the matching phase of the process. A similarity score between the template and the captured sample is checked against an operating threshold and a

decision outcome is reached. Different biometric operating systems may have different outcomes such as verification or identification or others, depending on the application. More detailed information about the operating thresholds is discussed in the next section.

2.3 Matching Scores and Thresholds

Traditional biometric systems assign a matching or similarity score for every attempted authentication. The degree to which a unique biometric template from the enrollment database matches the captured biometric sensor reading produces a matching score. Matching scores lie somewhere between the closed interval [0,1], where zero is a nonmatch and one is a full match. An established threshold level between zero and one determines if an authentication attempt is either accepted or rejected. This operating threshold is very important because it ultimately determines the effective FAR and the FRR. If the threshold were permissive of maximum error, then every authentication attempt would be accepted, including both genuine and impostor attempts—clearly an undesirable result. If the threshold were set to permit zero errors, nearly every authentication attempt would be rejected, resulting in severe system slow down—equally unacceptable. Therefore, the operating threshold for automated biometric systems must be maintained between these two extremes to ensure the lowest possible FAR and FRR.

The DET and ROC curves illustrate this inherent tension in automated biometric systems. Both the United States and Europe have established standard FAR's for automated biometric access systems. For example, the FRR when the FAR is fixed at .1%, expressed as $FAR_{.001}$, is a standard requirement for automated biometric systems at European border control checkpoints [14]. This is because many of the automated biometric systems in operation are typically designed to meet a security objective such as preventing impostors or watch-listed individuals. The United States, too, maintains specific Personal Identity Verification (PIV) standards for government

entities and industry through the Federal Information Processing Standards (FIPS) [15, 16]. Approved vendor manufacturers are required to pass standardized tests of biometric performance for operating biometric systems. FIPS establishes benchmarks for all federal employees and contractors attempting to gain access to government sites in the United States.

2.4 Operating Limits and Problems

These standardized operating thresholds have proven to be robust in automated biometric security performance. However, automated biometric checkpoints are subject to imperfect real-world operating conditions such as lack of adequate illumination, subject movement, poor sensor reads, operator or staff error, etc. As with other engineering fields, the error minimization is key. Another way to consider this problem is to recognize that to properly identify or verify individuals and—at the same time—prevent impostors from gaining access, the system is subject to a certain amount of “friction”.

In the United States, the FRR has been trending downwards since 1993, while still maintaining the prescribed FAR [17]. (See Figure 2.5 below). This is due in large part to the increased use of multimodal authentication systems. Multimodal biometric authentication—traditional biometric modalities coupled with newer biometric technologies including behavioral biometrics and distanced biometric measurements—virtually guarantee a low FAR and a decreasing FRR. Importantly, this guarantee is predicated on increased data extraction from both voluntary and involuntary sources. Multimodal biometrics are examined further in section 4.2.

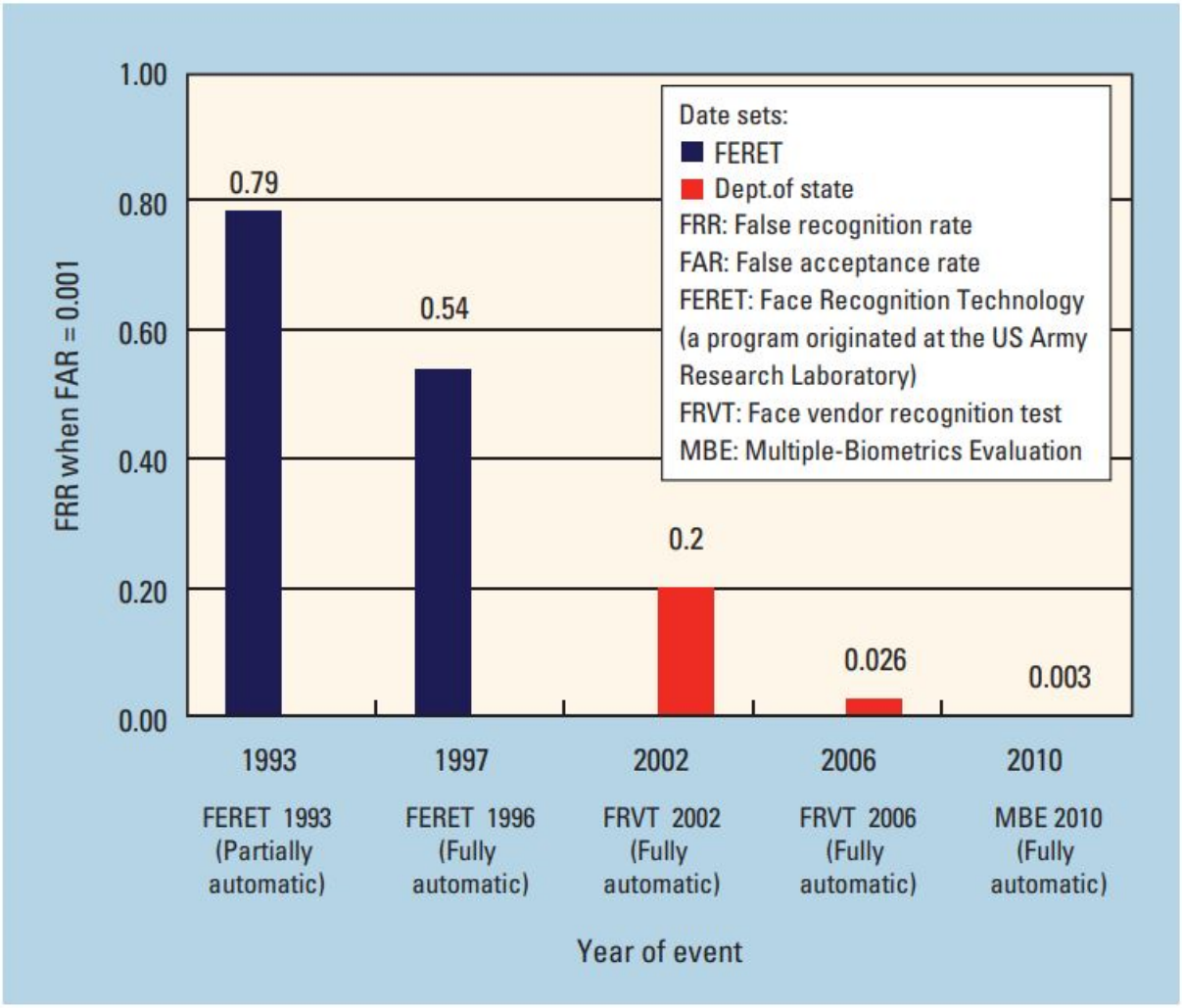

Figure 2.5: Automated face matching using full-frontal images [17]

2.5 Continued Biometric Data Extraction

It is well documented in the academic literature and industry that unimodal biometric systems (those utilizing a single biometric trait: iris, fingerprint, facial scan) are insecure compared to multimodal authentication systems [18]. To maintain broad biometric robustness, it is likely that more and more forms of human biometric data will be required for this purpose. Increased variety of identifying biometric data may help to maintain a low FAR and decreasing FRR. However, this

necessarily increases the amount of processed information, which may reduce operating speed of the authenticating device, which is examined later.

Moreover, the numerous ethical issues surrounding the extraction of PII at a distance—through various surreptitious or overt means—remain unresolved. The critical point to recognize, however, is that—irrespective of any ethical quandaries—automated biometric systems must continue to capture increasing volumes and varied types of PII to remain relevant or secure. The mandated FRR and FAR standards virtually ensure this fact. Comprehensive participation in civil society and international travel will almost certainly require increased collection of human behavioral biometric data at scale. Already, numerous countries have issued biometric passports for their citizens for travel abroad. Worldwide as of 2017, one-hundred twenty countries have issued biometric passports [19].

In the next chapter, various distanced biometric technologies are presented. These systems are noteworthy because they have become a significant contributor to different industries and represent a large body of research. These industries include healthcare, government and law enforcement, commercial travel, immigration control, consumer electronics, and many others. Moreover, the overall pervasiveness and shifting cultural attitudes toward the technology make the examination of its engineering aspects relevant.

III. DISTANCED BIOMETRICS

3.1 Identification from afar

Much research has been conducted into distanced biometric measurement. The development of gait biometrics, for instance, has advanced rapidly. Research utilizing Wi-Fi signals to recognize and successfully classify the unique frequency signatures of human beings has been demonstrated in both Line of Sight (LoS) and Non-Line of Sight (NLoS) scenarios. Utilizing the Doppler shift effect, researchers were able to determine not only the identity of the participants behind walls but were also able to successfully draw inferences about the participants' state during the experiments [20]. The experiments produced unique signatures for the states of walking, sitting, falling, and dragging one leg; all accurately classifiable by machine learning algorithms. This technology has been spearheaded for the medical industry and elderly care research. Its parallel application in the biometric security sphere has also been thoroughly studied.

Additionally, researchers have been able to identify human beings through unique dielectric signatures. Through a clever capacitive sensing technique, researchers were able to assign biologically unique frequency signatures to each individual and compare them [21]. The subjects were measured stationary in front of a capacitive metal plate at a specified distance. Since each human body's composition is specific to that individual, the relative differences in these capacitive measurements were enough to distinguish between them [21]. Other research has shown the unique patterns associated with human function such as brain wave patterns and breathing. [22]. Indeed, it appears that though much of human physiological function is largely similar, it is continually proving itself unique enough for differentiation. Human beings can be easily identified, classified, assessed, and authenticated at a distance by a host of biological measures.

3.2 Behavioral Biometrics

Another emerging sub-field in the area of biometrics is known as behavioral biometrics. This research springs out of other research areas such as kinesiology, behavioral science, and the like. The research is centered around identifying the unique biometric features of a persons' movement or liveness. The possession of a tracking device such as a cell phone, smart watch, or other biometric wearables can assist with this process. Accelerometer and gyroscopic data can be captured from the devices to form a behavioral profile with a distinct human signature [23]. Even the way in which one holds a phone to one's ear is unique to that individual. This technology is viewed as a security improvement for biometric research. Passwords, pin codes, and other forms of forgettable authentication have been found to be more easily compromised than behavioral biometrics. Multimodal biometric systems that utilize gait biometrics in this way are far more secure because a possible adversary would have significant difficulty mimicking the movements of an authentic user; especially if the authentication is employed on a continuous basis as is proposed for many of these schemes [24]. There are many possible implementations of this technology and consequences of its use. Many other forms of multimodal authentication already exist in spaces such as information and cyber security.

Behavioral biometrics can take on a myriad of forms and the list of behaviors is growing. Figure 3.1 displays various modalities from which a behavioral biometric profile can be generated. Voice, gesture, and gait are just some of the unique traits that can be accurately classified and linked to a single individual in real-time. Likely, more modalities will emerge as researchers and engineers devise clever ways to distinguish one person from another.

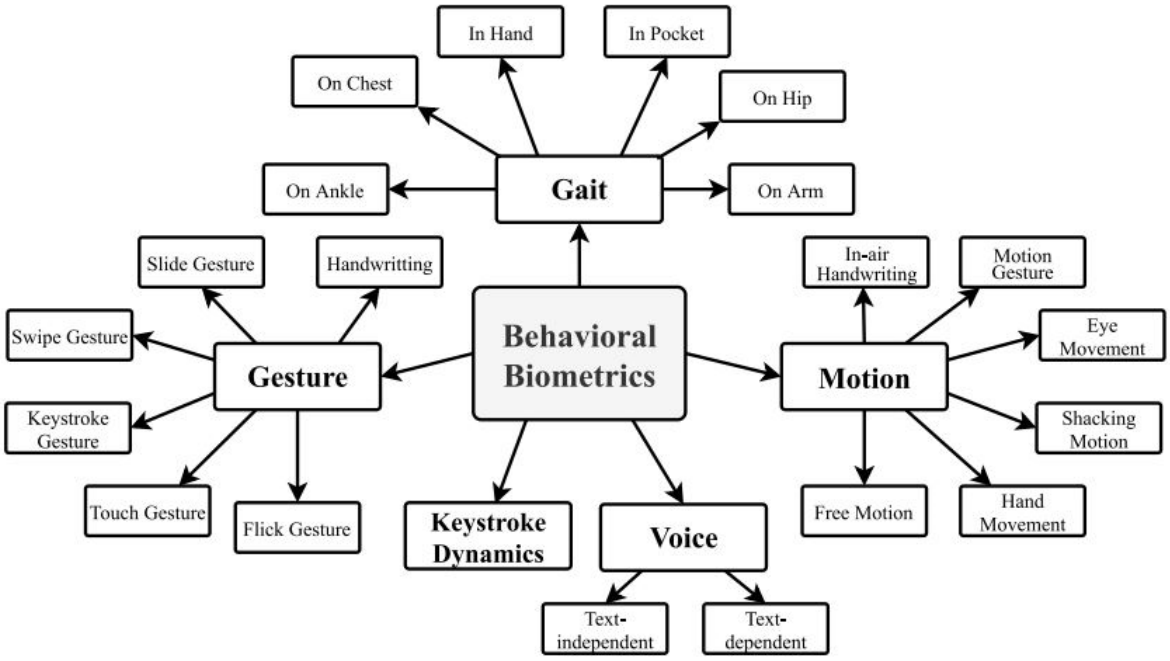

Figure 3.1: Behavioral Biometric Modality Chart [25]

3.2 Intent Biometrics

Research pertaining to intent biometrics is also tied to the behavioral sciences and utilizes some of the same algorithms employed for other biometric regimes. Specific human indicators such as perfusion of facial blood, body and localized facial temperature, gait changes, and other movements, can be measured and tracked in airports, border crossings, and other potential high value target areas [26]. Unlike classic biometric screening, which seeks merely to assess one's identity or authenticate an individual, the biometrics of intent seeks to infer what a person is about, that person's itinerant plans, that person's emotional state, etc [27]. It works within the continuous multifactor authentication framework in which a traditional physiological parameter—facial image, fingerprint, iris scan, etc.—is processed alongside a real-time additional behavioral parameter—heart rate, sweating, galvanic skin response, breathing rate, gait movements, gestures, etc. These measurements—taken at a distance—can be fused with more authenticating factor

streams such as cell phone activity metadata or location services tracking [28]. All this information can be synthesized and assessed to create a predictive behavioral profile based on probabilistic outcomes. Credit rating systems, predictive policing, and healthcare administration are other areas in which this technology has been implemented.

3.4 Efficiency and Security

It is apparent that the high throughput volumes observed at airports, borders, and other areas of immense security concern necessitate the development of multimodal biometric authentication technology [29, 30]. Globally, many airports have already deployed automated biometric authentication technologies to aid in efficient transportation service for frequent travelers. Iris and fingerprint scans are quickly becoming the norm. Manual passport identification procedure and other forms of 'hands on' authentication are steadily being eliminated. These evolving technologies and processes may—under the aegis of efficiency and secure authentication—appear as an absolute necessity in the future. Increasing security concerns, coupled with the need to efficiently process many individuals may broadly frame the discussion surrounding the social, ethical, and legal standards of behavioral biometrics in a direction that cannot be reversed. The possibility of an individual opting out of a biometric screening in the future may no longer be permitted under this evolving scenario. Or, as with other ubiquitous technologies such as cell phones, biometric bypassing may be technically possible but rendered wholly impracticable for successful daily living.

3.5 Expectation of Profiling Increases

As the security concerns surrounding traditional knowledge-based authentication technologies (passwords, PIN codes, tokens, etc.) continue to mount, the move towards a largely biometrically-based multimodal authentication scheme grows. If the capability of AI machines to

differentiate between biological signatures persists, then it is not unreasonable to expect that these various measurements will be incorporated into a larger personal biometric profile. In some regions of the world, this is already the case. A unique dossier of biometric traits may quickly extend far beyond a mere fingerprint or facial scan. Soon, it may include breathing rate, unique personal habits, brain wave function, and genetic information. Coupled with internet browsing history, payment history, location services data, social networking activity, and other metadata insights, a fine-grained resolution of human biometric identification and behavior is emerging.

In the following chapter, some of the techno-social problems that have arisen from the development of biometric technology are examined. These are complex and interesting problems that, in some cases, are unique to the field of biometrics. In other cases, though, these problems overlap with other engineering fields such as computer security. Teasing out the technical features of the various problems is both challenging and not altogether straightforward. Like many engineering problems, the achieved solution arrives in the form of a trade-off. In the case of automated biometrics, understanding exactly how and why the trade-offs occur is vital to understanding their wider social import.

IV. PROBLEMS IN BIOMETRICS

4.1 Cancelable Biometrics

A particular problem that has led to some novel work in the field is the problem of safe-guarding PII from so-called inversion attack. Some convolutional neural networks (CNNs) could be invertible via their outputs. In this case, the raw biometric data that form the input templates of the system have been shown in certain cases to be an exploitable vulnerability. Unlike passwords or token identification systems that can be reset, raw PII utilized in machine learning-based biometric regimes may not be recoverable if compromised. This is a significant biometric weakness that requires reform.

One solution to the problem of inversion attack is what is known as cancelable biometrics. Under this scheme, raw biometric inputs are intentionally distorted in such a way that renders recovery of the original templates impossible. Cancelable finger vein recognition systems are proving promising in this regard [31]. Deep learning finger vein template generation algorithms have been shown to be an effective means of securing PII. However, one trade-off is a decrease in the accuracy of the finger vein reads for an increased protection in the form of cancelable biometrics. As with many technologies, engineers must achieve a balance of interests to produce a well-rounded and effective result.

4.2 Multimodal Continuous Authentication

A significant technological hurdle that is an open area of research is the problem of achieving continuous biometric authentication. Past unimodal schemes have achieved remarkable accuracy but have suffered from numerous security flaws since they are reliant upon a single authenticating event: an iris scan, a fingerprint, a facial scan, etc. They are insufficient for safeguarding PII as well as preventing impostor intrusion. Numerous system flaws have been

exposed through various spoofing attacks, smudge attacks, heat attacks, and other sophisticated hacking techniques. Consequently, multimodal systems have come to the forefront of research and development. Broadly speaking, the vision of a robust biometrically-based security protocol has transitioned from a one-time user authentication event (iris scan, facial scan, keystroke, gesture, etc.), to a system of continuous authenticating events in which the user' behavioral biometrics are constantly assessed and validated. Indeed, it has been shown that mobile device intruders could perform more than 1000 tasks under knowledge-based authentication schemes but only achieve one task on a mobile device under a multimodal biometric method [25]. Much research has focused on harnessing the streams of cell phone data captured via the phone's embedded sensors [25]. Accelerometers, gyroscopes, and magnetometers are standard features of most cell phones in active use today. Programs have been written to document the unique patterns of movement, voice, gestures, and the like, of individual users using these embedded sensors. If this behavioral biometric information, combined with other certifying data can be used to passively authenticate subjects continually, then the authenticating system will have hardened its security profile and increased efficiency. Instead of a one-time authenticating event, the unique habits of the user are enrolled into the system and form the authentication templates in the database.

Part of the evolving challenge with this model is that continually monitoring biometric information requires overcoming numerous technological hurdles. One problem is that continuous monitoring consumes significant power from any mobile device. Some studies have shown the consumption can be as much as five percent of total power usage [25]. Even when the device is asleep, the monitoring programs consume more power than if they were not present at all. Another issue is the consumption of memory and computational resources [25]. Harvesting and coordinating this information requires large amounts of computing power that could be usefully

diverted elsewhere in the device. Despite these technical obstacles, it is likely that the multimodal system will dominate the biometric landscape of the future. The accuracy and effectiveness of a single biometric measurement is nearly always improved in combination with additional metrics.

The image below graphically represents the various modalities associated with the continuous authentication system. Each modality offers a unique way to verify and authenticate an individual. In fact, there are more biometrics than those listed in this chart. Coupled with different forms of behavioral biometrics, the multimodal system is capable of continuously authenticating individuals in real-time.

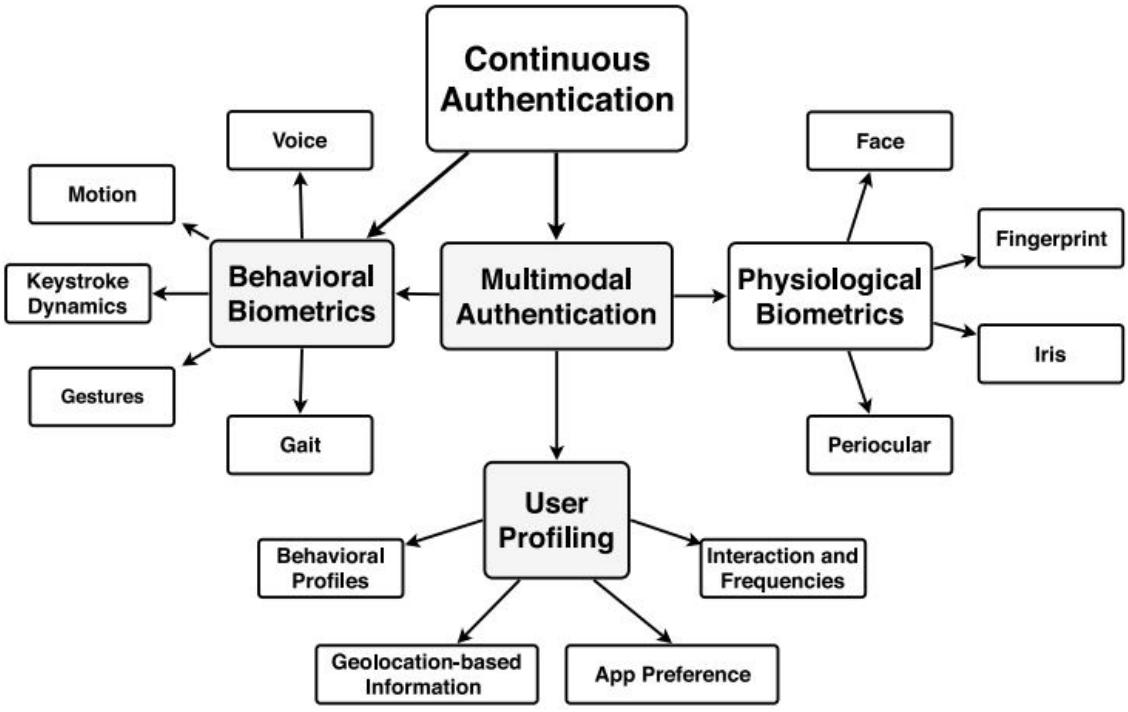

Figure 4.1: Continuous Authentication Modality Chart [25]

It is interesting to note here that many researchers have taken it as a stated engineering goal to create built-in technology for mobile devices that monitors behavioral biometrics in a covert way. It is important that the user remain unaware. This is sometimes referred to in the literature as

Zero-Effort Multi-Factor Authentication (ZEMFA) or also passive authentication. This is viewed as a security strength as well as a design improvement [24]. The continuous authentication model necessitates this action. Though it may seem strange or obvious to point out, it is important to understand that it would be an unreasonable request for users to constantly verify and authenticate themselves. Indeed, repeated authentication attempts from knowledge-based systems such as passwords already cause user frustration and are weak. The goal is to require "zero effort" on the part of the user. Therefore, the continuous authentication model appears to become an implicit element by default.

4.3 Algorithmic Bias

Another pressing techno-social problem on a broader level is the issue of algorithmic bias. Despite improvements in accuracy of facial recognition systems, it has been shown that biometric performance bias exists for certain demographic groups [32]. Female subjects specifically, as well as younger subjects (infants) have shown significant differences in bias when compared to other groups. Dark-skinned females, for instance, experience a lower classification accuracy for demographic attributes from facial images in some biometric systems. Other examples of biometric bias trends are appearing in the literature and the research is ongoing. The field is very new and requires more comprehensive study.

The initial survey of the problem of algorithmic bias appears to point toward the training data itself. Numerous studies suggest that algorithmic bias may be linked to the datasets and their country of origin. Algorithms developed primarily in Asia have been shown to recognize Asian individuals more easily, whereas algorithms developed in Europe have been shown to recognize Caucasian individuals more easily. In other academic disciplines, this is known as the 'other-race effect or own-race effect', which states that individuals are more easily able to recognize and

distinguish between members of their own race [32]. Similar effects have been observed regarding age identification. Some experiments that demonstrated these biased effects were based on small datasets, though not all. Larger datasets will likely lead to a more robust result with respect to accuracy and classification. However, the potential for these imbalanced effects to cause harm, even if unintentional, is significant. It should also be noted too that there is no evidence to suggest that algorithmic bias has been intentionally designed into the algorithms themselves. That is, there is no indication that the studied algorithms were maliciously contaminated to produce these biased effects. Rather, the algorithms reflect biased aspects of the data they were initially trained on.

Like the larger debate surrounding A/IS, the standards and benchmarks that govern the development of bias-free algorithms in biometrics remain in flux. No overarching consensus has been reached as to the definition of algorithmic fairness. Indeed, Drozdowski et al offer a succinct synopsis of the problem:

> The issues of fairness (including algorithmic fairness) are complicated from the point of view of the legislation—a somewhat deep understanding of statistics, formal fairness definitions, and other concepts is essential for an informed discourse. Furthermore, the ethical and moral perceptions and decisions are not uniform across different population demographics and by geographical location (see [191]). This reinforces an important dilemma regarding the regulation of automated decision systems—since many situations are morally and ethically ambiguous to humans, how should they be able to encode ethical decision making into laws? Once that issue is somehow surmounted, there also remains the issue of feasibility of technical solutions [32].

Some proposed solutions for mitigating problems associated with algorithmic bias include larger training datasets, multimodal biometrics, soft biometrics, and the biometrics of intent [33,

34]. These proposed solutions—as mentioned above—typically involve the fusion of multiple data streams to authenticate an identity. Unlike more rudimentary database classification and matching algorithms, multimodal approaches utilize other sources of identifying information to confirm an individual. Two-factor authentication is a parallel example of multimodal authentication in the field of information and cyber security. Paradoxically, since identification of traditional biometric characteristics such as a person's distinct facial features may be insufficient to ensure algorithmic fairness, the impetus for increased access to PII may be warranted. The pursuit of an equitable, fair, and comprehensive framework for biometrics may require the compromising forfeiture of some degree of personal privacy. Increasingly, as mentioned previously, there is significant research interest in biometric systems that identify and authenticate an individual by certain behaviors. Furthermore, the basic aim of identification and authentication of individuals has shifted over time to documenting—and in some cases predicting—more complex human behavior. The laudable and reasonable goal of continuing to ensure system-wide fairness may in fact lead to extraction of PII well beyond mere physical appearance. It may involve further documenting unique behavioral characteristics and traits over long periods of time. Authenticating who a person is may be less relevant or valuable than predicting their probable habits and tendencies.

In the next chapter, some of the ethical consequences of biometric technology are examined. As chapter V makes clear, the problems and risks that biometric technology presents are challenging and complex. The inherent tension between algorithmic fairness and personal privacy is an example of this type of difficult problem. These problems are not merely engineering hurdles to be overcome either. They have far more nuance. And many more biometric problems exist that are not listed in this research. As with all technological implementation, there is bleed over into other parts of society and culture.

V. ETHICAL CONCERNS

5.1 Irrevocability and Totalization

Like many formulations on the ethics of biometric security and other adjacent technologies, there exists a tendency to catastrophize about a future that has not yet arrived. Much has been written on the subject and the research needs to continue. It is always best to privilege present facts over distant speculation. But what seems to be consistently overlooked is the irrevocability and totalizing effect of automated biometrics. As with the electric grid, wireless communications, and nearly every other form of necessary civil infrastructure, a return to some prior primitive technological state is an out-and-out impossibility. Disconnection from large-scale power sources or the internet would wreak havoc for society, triggering vast amounts of human suffering and disruption. Many human beings are slavishly dependent on the reliability and efficacy of modern machines, including automated biometrics. If it is true that once a specific engineering technology is widely adopted and thereby made effectively irrevocable until something more sophisticated manifests, then the consequences of mistaking momentum for progress is vital. Engineers, researchers, scientists, policy makers, and others are ethically responsible for the biometric future that is being erected. Formal standardization of automated biometric technology will continue to guide industry and research but may ultimately prove insufficient at safeguarding PII or preventing other harms. The need for informed and potent independent oversight cannot be overstated. The United States to date has no regulating body to oversee the development of this important technology.

As discussed, due to the predominance of multimodal authentication, there already exists a tendency toward increased extraction of human biometric data, which is controversial. Presumably, this will make the biometric future more secure but with some caveats. Indeed, it has

been argued that much of the deployed biometric screening technology is operating in good faith, not in service to some misguided form of surveillance or repressive control. India's government, for instance, has issued over 1.2 billion biometric identification cards through its Aadhaar program, the world's largest biometric identification program [35]. It was developed as an essential governmental service distribution program. Aadhaar has been the subject of many legal and political arguments as well as the source of land disputes, fraud, and abuse. It has also, inarguably, provided millions of residents with essential benefits that they might not otherwise have received. As with many powerful technologies, the results are mixed.

5.2 History

Looking back, engineering standardization and codification has done much to legitimize and justify existing technological infrastructure. New ethical norms, too, came about alongside these innovative technologies. Others were torn down or withered away as older technology was steadily replaced. Biometric technology is currently undergoing this same process. As it proceeds, the request to forego identification, assessment, and authentication at a distance via intelligent algorithms and behavioral biometrics is growing increasingly unlikely. In the United States and elsewhere, the right to privacy has collided with deeper more entrenched security concerns of the state. Typically, these state concerns are only further bolstered by the process of standardization despite any wayward ethical objections. This slow eradication of ethical privacy contributes to the societal sense that biometric intrusion is—in day-to-day practice—insurmountable; that it is an integral, necessary, and natural part of a common shared reality; when in fact it is highly contrived, supported by standards and norms, funded, researched, and sanctioned by formal organizations and governments. Despite all of this, biometric technology is not yet irrevocable to the degree that entrenched technologies like electrical power are.

If tomorrow for example, in the United States, automated biometrics were severely hampered for whatever reason, society would probably hemorrhage greatly but would eventually recover. Citizens are not as reliant upon biometric systems as the electric grid. They might one day be, however. One of the most corrosive effects of increasing biometric intrusion is the sense that it is unavoidable, that resisting it will make little difference in the end. The appeal of granting unfettered access to the streams of biological data that are flowing from everyone is compelling. Opening-up biometrically is rewarded in society through increased convenience and a certain sense of technical sophistication. But as the privacy window shrinks, simply moving about the world becomes a scrutinized and documented event by default. Automated biometrics contribute significantly to this growing phenomenon.

Perhaps future historical texts will document a bygone era in which human identity and behavior was truly ephemeral, where events and temporary missteps might be forgotten in the ether instead of classified, assessed, and archived. Interestingly as an aside, the right to be forgotten has been vigorously debated in many arenas globally and has only recently come under consumer protection in the European Union via the General Data Protection Regulation (GDPR) in 2018 [3]. Private information that is released to the public is difficult to control or eliminate. An interesting, related question for debate is whether one's unique biometric signature ought to be formulated as a protected privacy right. Is the peculiar way in which one shuffles along in a busy train station an inviolable portion of one's identity and therefore safeguarded in the same way as other personally sensitive information? Should these bio signatures be treated in the same way as passwords and pin codes, secreted and protected from external intrusion? Or are these minute electrical measurements about a person merely a small slice of the enormous biometric pie available to all?

Despite the ethical qualms, there is little doubt that automated biometrics will greatly alter the future technological landscape, however it is deployed. The development of the technology and its application will be reflective of the local, state, and regional ethics of the future era. For this reason, it is imperative that automated biometric standards as well as the enforcement of those standards be held to a high ethical bar. It remains to be seen whether western states will be able to adequately balance the commercial drive towards automated biometric ascendancy with the reservations of concerned citizens. The technology could, in certain circumstances, function as a check against governmental abuse instead of serving as a surveillance tool to repress dissent or predict behavior. The camera might be turned in the opposite direction so to speak. It could directly serve the interests of citizens if implemented correctly. More likely, however, powerful state actors and industry leaders will pave the way. In any event, the ethical implications and technical frameworks of automated biometrics are still pliable enough that the outcomes are not completely fixed. In the next chapter, we provide some concluding remarks about biometric technology and its attendant consequences for the future.

VI. CONCLUSIONS

This work explored a two-part question. The first question considered the recent automated biometric engineering standards that have shaped and molded the field into its current condition. A comprehensive approach was utilized to examine various technical aspects of automated biometric research, the existing standards governing the technology, and some of the unresolved engineering problems. See Section 6.1 Technical Characteristics for a succinct summary of these issues. The second question contemplated some of the ethical and social dilemmas brought about by both the standards themselves and the nature of automated biometrics. See Chapter 5 Ethics for a detailed discussion of privacy, totalization, irrevocability, as well as other ethical issues. Some closing ethical observations can also be found in Section 6.2 Future Considerations.

6.1 Technical Considerations

The field of biometrics is in its developmental infancy. Like emerging technologies of the past era, automated biometrics is experiencing a turbulent period of rapid growth and research. In conjunction with this growth, inevitable disruptions with existing norms and other technologies have elucidated societal and ethical concerns that are not easily resolved. The right to privacy, algorithmic bias, biometric security and vulnerability, the potential for abuse, and the like, are recurring issues that can be found alongside any burgeoning technology. In spite of this, good faith efforts have been put forth to erect standards and norms for biometrics that harmonize and successfully integrate it with existing legal and technical standards. The GDPR in the Europe Union is a good example of this attempt.

Public tolerance of automated biometrics in the United States and elsewhere appears to be becoming widespread, though some communities are reticent to whole heartedly integrate the

technology into their daily lives. Others are leaping at the opportunity to open-up biometrically. Watches, cell phones, and other portable devices provide troves of biometric data that can be sifted by deep learning algorithms and programs, much to the benefit (or detriment) of the user. The sophistication and convenience of biometric technology is extremely enticing at the individual level. Moreover, the totalizing effect of continuous authentication technology sets up a situation in which distanced biometric measurement is accepted uncritically as the default mode.

Biometric evaluation and assessment metrics have improved dramatically since the technology's inception. Much of that improvement has largely been driven by a multimodal biometric approach. These systems have demonstrated superior robustness when compared against antiquated unimodal systems [18]. As a consequence of the multimodal approach, the FRR has decreased from seventy-nine percent in 1993 to .3 percent in 2010 when the FAR = .001, an almost 80 percent reduction over a period of 17 years [17]. (More recent data for the post 2010 period was not available regarding these rates). Currently, it is unknown whether the FRR will continue its greater than exponential rate of fall toward zero. (See Figure 6.1 next page).

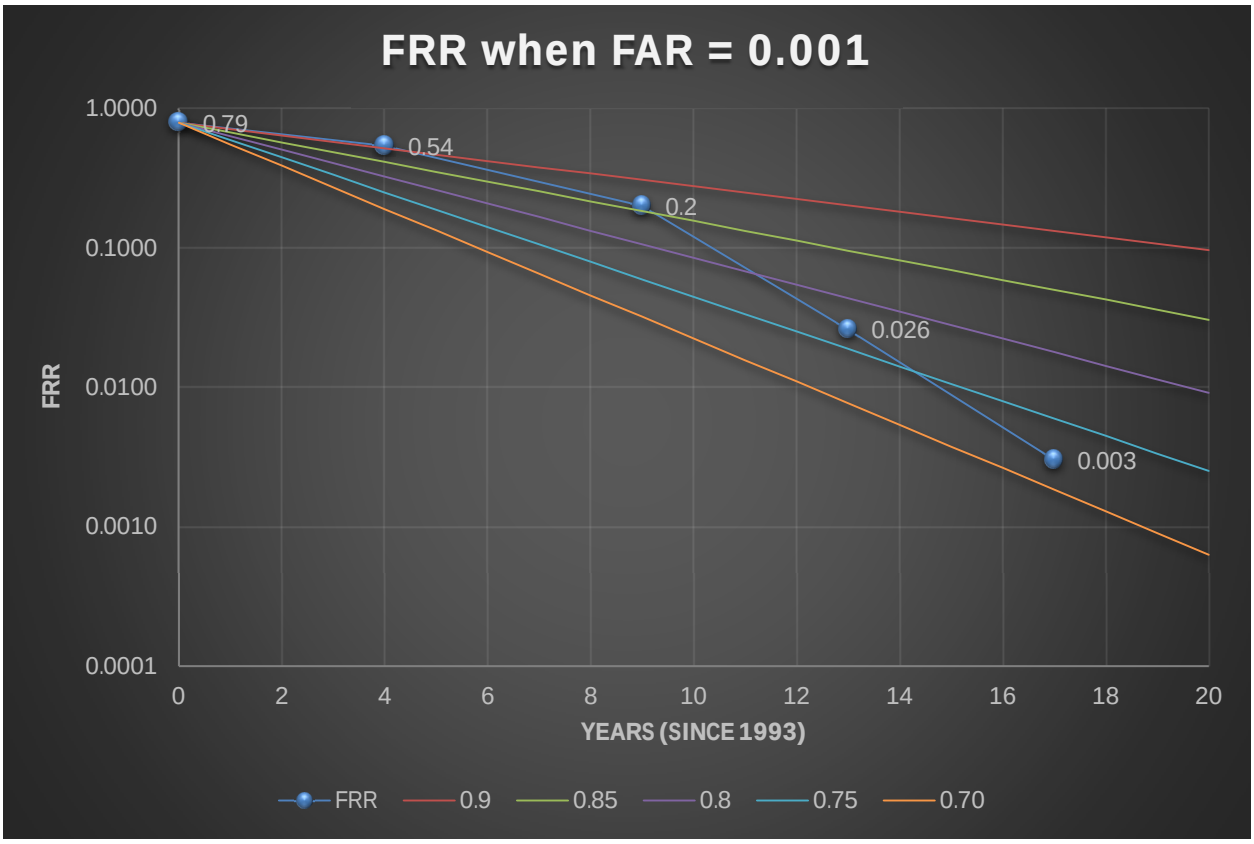

Figure 6.1: NIST data with logarithmic scale (See Figure 2.5)

Some related questions for future research might be: What are the associated costs (financial and otherwise) of achieving such a low FRR by these methods? Are there ways in which FRR's of .3 percent or lower could be attained while also keeping the FAR at its present level without resorting to an increase in volume and variety of biometric data? At what point does the amount of data acquired for this purpose produce a diminishing return?

As it stands, the research indicates that increasing the volume and variety of available data can lead to a more accurate and secure biometric system. This has led researchers and engineers to formulate a continuous multimodal authentication model. It pairs traditional identifying biometric traits (facial, iris, and fingerprint scans) with verifying behavioral biometric traits (gait, gesture, motion, and voice patterns). Among the many continuous authentication models proposed, a popular and feasible one utilizes embedded cell phone

sensors: accelerometers, gyroscopes, magnetometers, and the like. These sensors work in tandem to create a passive biometric authentication system via machine learning [23]. By capturing the data passively, the user is automatically verified and authenticated with minimal disruption. If the continuous authentication model becomes as ubiquitous and commonplace as current cell phone usage (which seems likely), then capturing increasing forms of private biometric data may be required to maintain robust security and efficiency performance.

In this way, voluntary participation in civil society may also be predicated on the involuntary or unwitting surrender of private biometric data. Indeed, biometric profiling, in its current form—if taken to its logical conclusion—may result in extensive, integrated personal dossiers. China, for instance, has already deployed its own sophisticated profiling system and have provided a workable model for others to follow suit [36]. At present, China ranks as the most biometrically invasive country on earth [36].

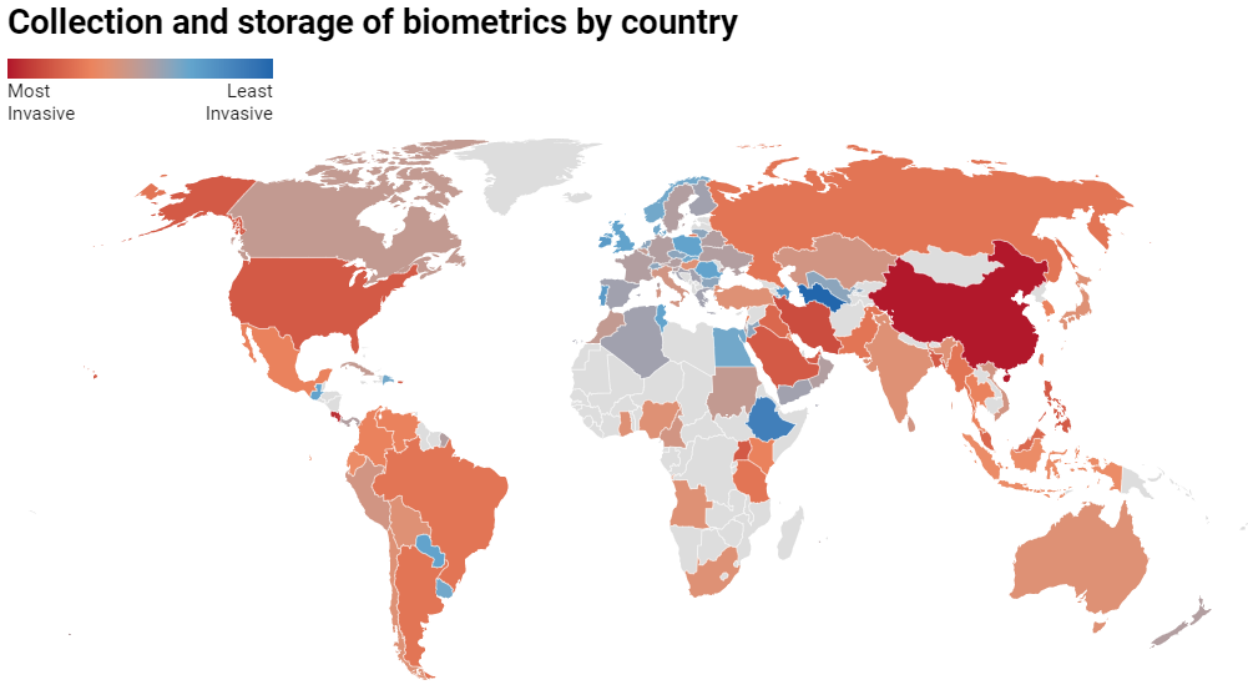

Figure 6.2: Worldwide Biometric Invasiveness Map [36]

The United States too is not far behind in its biometric invasive ranking at number four, at least according to one researcher [36].

It is conceivable that future dossiers may include identifying biometric features and behavioral records well beyond our current conception. At present, the four most well-researched and developed biometric technologies are fingerprint, facial recognition, iris recognition, and genetic testing. However, as has been demonstrated, there is increasing research and commercial interest in other innovative distanced biometric measurement techniques. These technologies are advantageous from an efficiency and effectiveness standpoint because they can be deployed covertly. In fact, as has been shown, this is an important engineering goal for researchers that work with ZEMFA technology.

At the institutional level, biometrics is gaining increased momentum because of its marked efficiency, efficacy, and manner of control. The ability of large governmental institutions to provide benefits and services to large populations using automated biometrics is unprecedented. As mentioned earlier, India's Aadhaar program to date serves over one billion users. Some biometric proponents point to the growing potential of the technology to aid underserved communities that are struggling. Wireless fall detection technology in elder care scenarios is a pertinent example in this context [20]. Biometric technology has the powerful capability to serve clients in a positive manner at scale.

At the same time, however, the rapid capability of governments and private corporations to monitor the habits and behaviors of private citizens without their consent is also unprecedented. The technological barriers that once served as a bulwark against privacy violations have been summarily removed. Though many technical challenges remain for biometric engineers, there is little left that cannot be accurately measured and understood from a

distance. The adoption of standards and regulations have helped somewhat to check against ethical violations but are largely toothless in the absence of independent regulating bodies. As was noted, the United States has no regulating agency to guide the development and implementation of automated biometric technology.

6.2 Future Considerations

What is clear is that the biometric groundwork that is being laid today is unlikely to be to unmade tomorrow. For this reason, the tendency of biometric technology to flow in one direction will make today's engineering and standardization decisions that much more critical when considering the future impacts. The FAR's and FRR's of the future are likely to improve but with some caveats. It is an open question as to whether it is even necessary to continue to improve these rates if that improvement is purchased at tremendous social and ethical cost. Biometric algorithms will almost certainly improve with time, and the FAR will fall below current operating levels. This will likely be hailed as a security improvement by industry. Biometric algorithms may even improve to such a degree that the institutionalized fixed FAR requirement will be justifiably lowered from $FAR_{.001}$ to $FAR_{.0001}$ or even lower. If this happens, the operating threshold will shift as a result, simultaneously altering the FRR in the process. (See figure 2.1, 2.3). This change would further serve to justify increased biometric data extraction for the multimodal system to ensure that the FRR not disrupt operational flow.

Since both metrics can never reach zero, the question then becomes how low is low enough for both rates? Is there a point at which enough requisite and varied biometric data has been collected and fused to meet existing security requirements for most major systems: airports, border control checkpoints, banks, etc? Has that level already been attained? Is it worth pursuing further? Of course, much of this discussion may be moot. CBP—as mentioned earlier in section

1.2—has not felt the need to justify the use of biometric facial recognition technology against its own citizens at the border [7]. The data is collected and stored for potential future use. Certainly, multimodal biometric data is useful for purposes other than simple identification and verification, which is why it is vitally important that strict limits are adopted and enforced. In the absence of sufficient regulation or some other countervailing force, it is predictable that automated biometric technology will continue its powerful ascent and ethical concerns will—by and large—be ignored. As was mentioned in the introduction, the United States remains in a significant legislative lag in relation to biometric technology. No overarching government body is overseeing the development of automated biometrics or even artificial intelligence generally. As a result, industry as well as other biased interests produce their own sets of norms and practices which privilege an unbridled dissemination of the technology coupled with a tepid consideration of the ethical aftereffects.

Importantly, like other technological achievements, the slow but steady pace of biometric development has allowed for ample positive conditioning among large groups of users, particularly among teenage users in the United States and elsewhere. Repeated and sustained contact with biometrics fosters an indifferent and unremarkable attitude toward the technology. It also promotes a sense of dependency. Thus, sustained technological exposure rates contribute meaningfully to a societal and ethical sense of biometric normalization. This process is spurred along through ubiquitous and frequent biometric encounters that form a pathway toward ethical default for the individual. What legitimate choices are truly available to the individual who seeks to avoid biometric scrutiny and finds the technology invasive? More and more, the only realistically available option is to begrudgingly accept the situation as it stands and move on with one’s life. In other words, the best option is really no option at all.

As the varied streams of biometric data are brought online and integrated, the sturdier the system becomes. Technology of this scope and strength will not easily be undone. And perhaps there is little reason to undo it. In fact, undoing it at this point would probably be more detrimental than anything else. But nevertheless, diving headlong into an automated biometric future with minimal ethical consideration is unwise. Any culture that values privacy at all should proceed cautiously. The technology ought to be properly governed and reigned in accordingly. What constitutes appropriate governance of such a powerful technology like automated biometrics is, of course, a question for vigorous and open debate. But that question is, oftentimes, not being asked. It is being avoided because it is a thorny question fraught with contradiction. Proper guidance of the technology requires nuance and understanding, not just rigorous wholesale improvement of automated biometric techniques. Renewed research into biometric engineering paradoxes (accuracy versus fairness, privacy versus public security, etc.) should be conducted. The standards and legislation are due for an update. If a reasonable biometric balance is not struck in this regard, then a power asymmetry will persist that may remain permanently. The engineers, scientists, policy makers, and researchers—those who understand at the deepest level the capability and innerworkings of automated biometrics—are the chief architects of the biometric future. They are tasked with the immense responsibility of duly considering the diverse perspectives of those that do not share their level of technological comprehension. If those concerns can be met, then perhaps a more successful and stable biometric future can be constructed.

REFERENCES

*Note: Of the first thirty-six cited references listed below, sixteen are IEEE publications. They are denoted with the * symbol for convenience. Additionally, during the course of research for this work, additional references were consulted that the reader may find informative. They are listed in a separate section below.*

1. * "IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being," IEEE Standard 7010-2020, IEEE Standards Assoc 2020 IEEE, May 2020, doi: 10.1109/IEEESTD.2020.9084219.

2. * "IEEE Standard for Biometric Open Protocol," IEEE Standard 2410-2019, IEEE Standards Association, June 2019, doi: 10.1109/IEEESTD.2019.8751181.

3. * Ayala-Rivera and L. Pasquale, "The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements," in *2018 IEEE 26th International Requirements Engineering Conference (RE)*, Banff, AB, pp. 136–146, Aug. 2018, doi: 10.1109/RE.2018.00023.

4. 116th Congress 1st Session, "Proposed Bill S. 847 – Commercial Facial Recognition Privacy Act of 2019" Blunt, pp. 1-15, [Online:] https://www.congress.gov/bill/116th-congress/senate-bill/847/text.

5. Illinois General Assembly, "(740 ILCS 14/) Biometric Information Privacy Act," Oct. 2008, [Online:] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

6. "Report 2019-01 of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection with the Use of Facial Recognition Technology," pp. 1-13. Feb. 2019, [Online:] https://www.dhs.gov/publication/dpiac-recommendations-report-2019-01.

7. "Re: DHS 2019-00001,DHS Data Privacy and Integrity Council," Center for Democracy and Technology, pp. 1-8, Feb. 2019, [Online:] https://www.dhs.gov/sites/default/files/publications/Center%20for%20Democracy%20%20Technology%20Comment%20DHS-2019-0001%20%28003%29.pdf.

8. "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update," pp. 1-50, June 2019, [Online:] https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf.

9. C. Busch, "Performance and Vulnerability Testing according ISO/IEC: overview and relevance," pp. 1-68, Nov. 2014 [Online:] https://christoph-busch.de/files/Busch-EAB-PAD-141117.pdf.

10. N. Poh, “Description of Metrics For The Evaluation of Biometric Performance,” in *BEAT: Biometrics Evaluation and* Testing, pp. 1-22, Aug. 2012, [Online:] https://www.beat-eu.org/project/deliverables-public/d3.3-description-of-metrics-for-the-evaluation-of-biometric-performance.

11. Biometrika, FAR and FRR curves, [Online:] http://www.biometrika.it/eng/images/farfrr.gif

12. Receiver Operating Characteristic (ROC) curve, [Online:] https://i.stack.imgur.com/VIb3C.png

13. Detection Error Tradeoff (DET) curve, [Online:]https://i.stack.imgur.com/JRIwr.png

14. European Union and European Agency for the Management of Operational Cooperation at the External Borders, “Guidelines for processing of third country nationals through automated border control,” Warsaw: FRONTEX, pp. 1-62, Sept. 2016, [Online:] https://frontex.europa.eu/publications/guidelines-for-processing-of-third-country-nationals-through-automated-border-control-vm9d3t.

15. Computer Security Division, Information Technology Laboratory, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” National Institute of Standards and Technology, NIST FIPS 201-2, Aug. 2013, doi: 10.6028/NIST.FIPS.201-2.

16. P. Grother, W. Salamon, and R. Chandramouli, “Biometric Specifications for Personal Identity Verification,” National Institute of Standards and Technology, NIST SP 800-76-2, Jul. 2013, doi: 10.6028/NIST.SP.800-76-2.

17. B. Wing, “NIST Contributions to Biometric Technology,” *IT Prof.*, vol. 16, no. 2, pp. 38–44, Mar. 2014, doi: 10.1109/MITP.2013.89.

18. * A. P. Yazdanpanah, K. Faez, and R. Amirfattahi, “Multimodal biometric system using face, ear and gait biometrics,” in *10th International Symposium on Information Science, Signal Processing and their Applications (ISSPA 2010)*, Kuala Lumpur, Malaysia, pp. 251–254, May 2010, doi: 10.1109/ISSPA.2010.5605477.

19. Wikipedia contributors. Biometric passport. Wikipedia, The Free Encyclopedia. [Online:] https://en.wikipedia.org/w/index.php?title=Biometric_passport&oldid=1012059294.

20. * Y. Li and T. Zhu, “Using Wi-Fi Signals to Characterize Human Gait for Identification and Activity Monitoring,” in *2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, Washington, DC, USA, pp. 238–247, Jun. 2016, doi: 10.1109/CHASE.2016.20.

21. * J. Iqbal, M. T. Lazarescu, O. B. Tariq, A. Arif, and L. Lavagno, “Capacitive Sensor for Tagless Remote Human Identification Using Body Frequency Absorption Signatures,” *IEEE Trans. Instrum. Meas.*, vol. 67, no. 4, pp. 789–797, Apr. 2018, doi: 10.1109/TIM.2017.2789078.

22. * Rahman, E. Yavari, V. M. Lubecke, and O.-B. Lubecke, “Noncontact Doppler radar unique identification system using neural network classifier on life signs,” in *2016 IEEE Topical Conference on Biomedical Wireless Technologies, Networks, and Sensing Systems (BioWireleSS)*, Austin, TX, USA, pp. 46–48, Jan. 2016, doi: 10.1109/BIOWIRELESS.2016.7445558.

23. J. Maghsoudi and C. C. Tappert, “A Behavioral Biometrics User Authentication Study Using Motion Data from Android Smartphones,” in *2016 European Intelligence and Security Informatics Conference (EISIC)*, Uppsala, Sweden, pp. 184–187, Aug. 2016, doi: 10.1109/EISIC.2016.047.

24. * B. Shrestha, M. Mohamed, and N. Saxena, “ZEMFA: Zero-Effort Multi-Factor Authentication based on Multi-Modal Gait Biometrics,” in *2019 17th International Conference on Privacy, Security and Trust (PST)*, Fredericton, NB, Canada, pp. 1–10, Aug. 2019, doi: 10.1109/PST47121.2019.8949032.

25. * M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, “Sensor-Based Continuous Authentication of Smartphones’ Users Using Behavioral Biometrics: A Contemporary Survey,” *IEEE Internet Things J.*, vol. 8, no. 1, pp. 65–84, Jan. 2021, doi: 10.1109/JIOT.2020.3020076.

26. Shiqian Wu, Zhenghui Gu, Kia Ai Chia, and Sim Heng Ong, “Infrared facial recognition using modified blood perfusion,” in *2007 6th International Conference on Information, Communications & Signal Processing*, Singapore, pp. 1–5, 2007, Dec. 2007, doi: 10.1109/ICICS.2007.4449707.

27. * J. Chamieh, J. Al Hamar, H. Al-Mohannadi, M. Al Hamar, A. Al-Mutlaq, and A. Musa, “Biometric of Intent: A New Approach Identifying Potential Threat in Highly Secured Facilities,” in *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Barcelona, pp. 193–197, Aug. 2018, doi: 10.1109/W-FiCloud.2018.00037.

28. * E. Gilady, D. Lindskog, and S. Aghili, “Intent Biometrics: An Enhanced Form of Multimodal Biometric Systems,” in *2014 28th International Conference on Advanced Information Networking and Applications Workshops AINA-2014*, BC, Canada, pp. 847–851, May 2014, doi: 10.1109/WAINA.2014.133.

29. “TSA BIOMETRICS ROADMAP For Aviation Security & the Passenger Experience,” pp. 1-23, Sept. 2018, [Online:] https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

30. “Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies Report to Congress,” U.S. Department of Homeland Security, pp.1-43, Aug. 2019, [Online:] https://www.tsa.gov/sites/default/files/biometricsreport.pdf.

31. * W. Yang, S. Wang, J. Hu, G. Zheng, J. Yang, and C. Valli, “Securing Deep Learning Based Edge Finger Vein Biometrics With Binary Decision Diagram,” *IEEE Trans. Ind. Inf.*, vol. 15, no. 7, pp. 4244–4253, Jul. 2019, doi: 10.1109/TII.2019.2900665.

32. * P. Drozdowski, C. Rathgeb, A. Dantcheva, N. Damer, and C. Busch, “Demographic Bias in Biometrics: A Survey on an Emerging Challenge,” IEEE Transactions in Technology & Society. vol. 1, no. 2, p. 15, May 2020, doi: 10.1109/TTS.2020.2992344

33. * K. Ricanek and B. Barbour, “What Are Soft Biometrics and How Can They Be Used?,” *Computer*, vol. 44, no. 9, pp. 106–108, Sep. 2011, doi: 10.1109/MC.2011.296.

34. * T. J. Neal and D. L. Woodard, “You Are Not Acting Like Yourself: A Study on Soft Biometric Classification, Person Identification, and Mobile Device Use,” *IEEE Trans. Biom. Behav. Identity Sci.*, vol. 1, no. 2, pp. 109–122, Apr. 2019, doi: 10.1109/TBIOM.2019.2905868.

35. * S. M. Rafi, N. P. Kumar, and D. J. Kumar, “Survey for Interlinking of DNA Models with Aadhaar Real-Time Records for Enhanced Authentication,” in *2019 5th International Conference on Advanced Computing & Communication Systems(ICACCS)*, Coimbatore, India, pp. 208–211, Mar. 2019, doi: 10.1109/ICACCS.2019.8728512.

36. P. Bischoff, “Biometric Data: 96 Countries Ranked by How They’re Collecting It and What They’re Doing With It,” from www.comparitech.com, Jan. 2021, https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/.

Additional References

1. R. M. Bolle, S. Pankanti, and N. K. Ratha, "Evaluation techniques for biometrics-based authentication systems (FRR)," in *Proceedings 15th International Conference on Pattern Recognition. ICPR-2000*, Barcelona, Spain, vol. 2, pp. 831–837, Sept. 2000, doi: 10.1109/ICPR.2000.906204.

2. Igglezakis and D. Politis, "Digital forgetting in the age of on-line media: The forensics for establishing a comprehensive right to cyber-oblivion," in *2014 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL2014)*, Thessaloniki, Greece, pp. 274–279, Nov. 2014, doi: 10.1109/IMCTL.2014.7011147.

3. T. Hagendorff, "The Ethics of AI Ethics: An Evaluation of Guidelines," *Minds & Machines*, vol. 30, no. 1, pp. 99–120, Mar. 2020, doi: 10.1007/s11023-020-09517-8.

4. T. B. Kane, "Artificial Intelligence in Politics: Establishing Ethics," *IEEE Technol. Soc. Mag.*, vol. 38, no. 1, pp. 72–80, Mar. 2019, doi: 10.1109/MTS.2019.2894474.

5. M. M. Broman and P. Finckenberg-Broman, "Socio-Economic and Legal Impact of Autonomous Robotics and AI Entities: The RAiLE Project," *IEEE Technol. Soc. Mag.*, vol. 37, no. 1, pp. 70–79, Mar. 2018, doi: 10.1109/MTS.2018.2795120.

6. Kuleshov, "Formalizing AI System Parameters in Standardization of AI," in *2018 International Conference on Artificial Intelligence Applications and Innovations (IC-AIAI)*, Nicosia, Cyprus, pp. 51–54, Oct. 2018 doi: 10.1109/IC-AIAI.2018.8674446.

7. Etzioni and O. Etzioni, "Designing AI systems that obey our laws and values," *Commun. ACM*, vol. 59, no. 9, pp. 29–31, Aug. 2016, doi: 10.1145/2955091.

8. Vakkuri, K.-K. Kemell, and P. Abrahamsson, "Ethically Aligned Design: An Empirical Evaluation of the RESOLVEDD-Strategy in Software and Systems Development Context," in *2019 45th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, Kallithea-Chalkidiki, Greece, pp. 46–50, Aug. 2019, doi: 10.1109/SEAA.2019.00015.

9. K. Shahriari and M. Shahriari, "IEEE standard review — Ethically aligned design: A vision for prioritizing human wellbeing with artificial intelligence and autonomous systems," in *2017 IEEE Canada International Humanitarian Technology Conference (IHTC)*, Toronto, ON, Canada, pp. 197–201, Jul. 2017, doi: 10.1109/IHTC.2017.8058187.

10. R. C. Arkin, "Ethics and Autonomous Systems: Perils and Promises [Point of View]," *Proc. IEEE*, vol. 104, no. 10, pp. 1779–1781, Oct. 2016, doi: 10.1109/JPROC.2016.2601162.

11. “Independent High-Level Expert Group on Artificial Intelligence setup by the Eurpoean Union: Policy and Investment Recommendations for Trustworthy AI,” pp. 1-41, April 2019, [Online:] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

12. “IEEE Standard Ontologies for Robotics and Automation," in IEEE Standard 1872-2015, IEEE Standards Assoc 2015 IEEE vol., no., pp.1-60, 10 April 2015, doi: 10.1109/IEEESTD.2015.7084073.

13. Y. Mochizuki, “AI and IoT for Social Value Creation,” in *2019 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, Macau, Macao, pp. 99–102, Nov. 2019, doi: 10.1109/A-SSCC47793.2019.9056955.

14. Jain, B. Klare, and A. Ross, “Guidelines for best practices in biometrics research,” in *2015 International Conference on Biometrics (ICB)*, Phuket, Thailand, pp. 541–545, May 2015, doi: 10.1109/ICB.2015.7139116.

15. S. Cherry and A. Corley, “Bad vibes,” *IEEE Spectr.*, vol. 47, no. 1, pp. 60–62, Jan. 2010, doi: 10.1109/MSPEC.2010.5372505.

16. M. Trikoš, I. Tot, and J. Baj, “Biometric Security Standardization,” *2019 Zooming Innovation in Consumer Technologies Conference (ZINC)*, p. 4, May. 2019, doi: 10.1109/ZINC.2019.8769419

17. J. Preciozzi *et al.*, “Fingerprint Biometrics From Newborn to Adult: A Study From a National Identity Database System,” *IEEE Trans. Biom. Behav. Identity Sci.*, vol. 2, no. 1, pp. 68–79, Jan. 2020, doi: 10.1109/TBIOM.2019.2962188.

18. Rathgeb, C.-I. Satnoianu, N. E. Haryanto, K. Bernardo, and C. Busch, “Differential Detection of Facial Retouching: A Multi-Biometric Approach,” *IEEE Access*, vol. 8, pp. 106373–106385, June 2020, doi: 10.1109/ACCESS.2020.3000254.

19. Q.Xiao and M. Savastano, “An Exploration on Security and Privacy Issues of Biometric Smart ID Cards,” in *2007 IEEE SMC Information Assurance and Security Workshop*, West Point, NY, USA, pp. 228–233, Jun. 2007, doi: 10.1109/IAW.2007.381937.

20. X.Duan, C. Wang, X. Liu, Z. Li, J. Wu, and H. Zhang, “Ethnic Features extraction and recognition of human faces,” in *2010 2nd International Conference on Advanced Computer Control*, Shenyang, China, pp. 125–130, Mar. 2010 doi: 10.1109/ICACC.2010.5487194.

21. X Yu, Q. Yang, R. Wang, R. Fang, and M. Deng, “Data Cleaning for Personal Credit Scoring by Utilizing Social Media Data: An Empirical Study,” *IEEE Intell. Syst.*, pp. 7–15, Feb. 2020, doi: 10.1109/MIS.2020.2972214.