

RESEARCH ARTICLE OPEN ACCESS

From Identification to Recognition: A Lesson for Biometric Technology From the History of Personal Identity

Emilio Mordini¹  | James L. Wayman² 
¹NORIA, Fiume Veneto, Italy | ²Independent Researcher, Pebble Beach 93953, California, USA

Correspondence: Emilio Mordini (emilio.mordini@noria-onlus.it)

Received: 31 July 2025 | **Revised:** 13 January 2026 | **Accepted:** 9 February 2026

Academic Editor: Reza Shahbazian

ABSTRACT

Throughout the history of automated personal identification, now called “biometrics” in some communities, there has been controversy over its implications for personal privacy and human dignity. This controversy has been deepened by equivocation regarding the philosophical concept of personal identity, the social concept of recognition of persons, and the forensic concept of person identification. These concepts of personal identity, recognition, and identification are central to Western literature, shared traditions, and our notions of “self,” so it is not surprising that technologies dealing with these issues would elicit controversy. The assumption of this paper is that greater understanding of the cultural meanings and nuances of these concepts is necessary to illuminate some critical aspects of the current ethical and policy debate surrounding biometric technology. Accordingly, we attempt to deconfound these core concepts by differentiating persons from attributes and labels from notions of self. We explicate two different but interrelated forms of identity and discuss their connection to recognition, identifiers, and identification. Clear definitions are presented for each of these concepts. With the intent of enlightening the complicated relationship society and individuals have with biometric technology, we discuss social risks and suggest that the complexities of identity and recognition have always been important in Western tradition, as illustrated in the Biblical story of Abraham and the Greek story of Odysseus. We conclude that biometric technologies, although not without risks, have a legitimate place in modern society for assigning identifiers to persons based on body characteristics and should not be understood as extending to the philosophical and religious foundations of personal concepts of self.

1 | Introduction

Society strives for person identification to enforce accountability, deliver entitlements, or, more recently, to enable commercial exploitation at the level of the individual. This has led to huge growth in automated personal identification technologies and personal information databases. Tension occurs because individuals strive to control identification of themselves by others—sometimes seeking to promote it for ego enrichment or attachment to entitlements, sometimes seeking to prevent it, preferring anonymity. Practitioners and policy makers regularly meet with opposition to personal identification technologies traceable

directly to these tensions. In this paper, we will seek to deconfound the related but distinct elements of person identification, recognition, identity, and “self” with the goal of forging a path forward through these tensions while acknowledging the legitimacy of societal and individual concerns over these technologies.

Identification requires, as the first step, the assignment of an identifier, which is a label to a record. Biometrics¹ can be used to facilitate this first step in person identification through assignment of identifiers based on characteristics of the body. Providing that the record pointed to by the identifier is sufficiently

This is an open access article under the terms of the [Creative Commons Attribution](https://creativecommons.org/licenses/by/4.0/) License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

Copyright © 2026 Emilio Mordini and James L. Wayman. *IET Biometrics* published by John Wiley & Sons Ltd.

informative, the person whose data provides the identifier can be said to have been “identified.”

The concept of recognition, however, seems somewhat different and weaker than identification. We often recognize people that we cannot name, tunes that we have heard but cannot sing, and flowers that we love but cannot clearly describe from memory. Recognition lacks assignment of a label pointing to a sufficiently informative record, and although recognition is a first step toward identification, it is not the same.

“Personal identity” is connected to these concepts but is of a deeper, more intimate nature. Recognition, assignment of identifiers, and identification can be done by others and about others, but identity, as a sense of “self,” is within the individual. The quest for personal identity is existential, at the philosophical and religious core of every person. The introduction of technologies for recognition or identification relates to, but does not fundamentally change, the personal quest for “identity” as knowledge of self.

Thus, identity, identifiers, identification, and recognition are four distinct but intertwined terms with broad importance to Western societies since the dawn of written history. The development of automated methods of human recognition beginning only 60 years ago [1, 2] has been seen to impact our historical understanding of these concepts, often represented as assisting government surveillance, violating privacy, allowing economic exploitation, or leading to government social and political control [3–6]. Technical papers have claimed that automated human recognition methods can allow others to determine “who I am” or “if I am who I claim to be” [7–11]. The claim of this paper is that human identity is not a concept that should be trivialized by implying that it can be determined or ascertained by the application of technology. In this paper, we reject the reductionist view that core issues of human identity can be resolved by the output of a technology. We look for a deeper understanding of the cultural meanings and nuances of identity, identifiers, identification, and recognition to illuminate critical aspects of the current ethical and policy debates surrounding biometrics.

The relationship between biometric recognition and the philosophy of personal identity has been previously explored by A. Kind [12], who argues, “...it would be a mistake to conclude that issues about biometric recognition should be seen as completely orthogonal to philosophical discussions of personal identity.” Although we agree with this statement, we contend that much of the opposition to biometrics comes from the mistaken idea that biometric recognition is completely parallel to personal identity.

In the first section, we will distinguish between recognition, identifiers, and attributes, arguing that recognition requires the application of a label (an “identifier”), which can be noninformative, or alternatively, might be linked to attributes of the entity recognized. Both identifiers and attributes can be transient, even if recognition endures.

In the second section, we will differentiate between the intertwined philosophical concepts of identity as “same” and identity as “self.” It is in the confounding of these two concepts that many of the concerns relating to biometrics emerge.

In the third section, we will discuss some of the risks associated with biometric recognition, including loss of privacy and

potential “digital discrimination” based on biometric attributes. We will argue that such risks accompanying deployment of biometric technologies may be unintentional and difficult to mitigate. Further, we will explore the risks to human dignity when the two concepts of “same” and “self” are completely severed.

In the fourth section, we will argue that the struggle between identity as “same” and as “self” is among the core narratives of Western thought, as illustrated in Homer’s *Odyssey* and the biblical story of Abraham. Moreover, we will suggest that identity, identification, and recognition refer to a wide spectrum of meanings, including metaphysical meanings connected to the notion of the sacred. The importance of human identity in Western civilization should not be trivialized through the implication that identity and identification can be equated with the output of a technology.

Finally, we will summarize the main lessons to be drawn from this article concerning the differences between recognition, identifiers, identification, and identity. Individual definitions for these concepts, emphasizing their distinctions, are summarized in Table 1. These themes deserve to be developed and explored further in future work, as they promise to have important implications for biometrics policy. While none of the ideas presented in this paper is in itself original, as the use of multiple references certainly indicates, we feel that bringing them all together in one paper makes an original contribution to the field of biometrics.

2 | Recognition, Identifiers, Attributes, and Identification

The term “recognition” is composed of the Latin bases “re” (again) and “(g)noscere” (know), so it simply means “to know again.” The question of “what constitutes knowledge” is perhaps philosophically intractable, but for the purposes of “recognition,” “know” means nothing more than to be able to acknowledge something as previously encountered. On further encounters, a tentative label or “identifier,” acknowledging the initial encounter, can be attached, as in “an item I have seen somewhere before.” “Recognition” as “being able to acknowledge something as previously encountered” need not tell us anything more about the object. A baby can recognize milk as previously encountered without knowing what it is called or anything about its chemical content. But once something is labeled (given an identifier), the baby can begin to assign attributes beyond “seen before.” If it is milk, they might assign the attributes “white liquid,” “tastes good” and “is warm.” Upon repeated encounters or closer inspection, they might understand that not all of those attributes apply to all encounters with the liquid. They may learn that milk has additional attributes (“can be cold”) not previously considered. They may therefore either adjust the attributes or consider further classifying the object (“cold liquid”). So for the purposes of considering identity, identification, recognition, and biometric technology, we can say that “recognition” is finding an identifier of an object. Although initially that identifier may point to no more information in the form of attributes than “previously encountered,” with additional encounters more information can be associated with the identifier for future recall.

Recalling attributes, which are always incomplete and often incorrect, can be seen as a subsequent process limited by what

TABLE 1 | Definitions.

Biometrics	The automated recognition of individuals based on biological and behavioral characteristics [13].
Identifier	Pointer to an entity or a record of attributes (possibly null) about an entity [14].
Biometric identifier	A pointer based on biological and behavioral characteristics sufficiently stable and distinctive over the time period and population of interest.
Recognition	Labeling an entity as previously encountered.
Biometric recognition	Use of automated technology to apply a stable and distinctive biometric identifier to an individual previously encountered.
Identify/identification	Find an identifier sufficiently informative for others to assign attributes to this entity.
Idem-identity	A label stable over time and application, allowing the linking of attribute records to a single individual within the population of interest.
Biometric identity	A sufficiently distinctive biometric-based label allowing linkage to attribute records of only one person in the population of interest.
Iipse-identity	Personal, potentially transient concept of self as different from others.
Biometric verification	A process supporting or denying a claim of an individual’s association with a record by comparing biometric attributes to those of the record.

we have previously learned about the object. The attributes alone might be used as an identifier (“white liquid that is good to drink”). At some point, we will have assembled an identifier informative enough that our meaning can be expressed to others, allowing them to connect the object to attributes acquired through their own experiences. If we teach the baby to use the identifier “milk,” the baby can express himself in a way that allows others to assign their own attributes of the substance. The white liquid will be “identified” in a way that others can infer its attributes from their own personal experiences. So “recognition” involves nothing more than labeling something as previously encountered, but “identification” involves being able to communicate a labeling sufficient for others to assign their own attributes to this object. The attributes assigned will depend not only on the object being described but also upon the person or organization assigning them.

When we transfer this idea to the identification of individual persons, attributes assigned will depend upon both who is assigning them and to whom they apply. The labeling identifiers might come from a different entity than the assignment of attributes, meaning that even if there is agreement on the identifier, there might not be agreement on the attributes. Although the list or “record” of attributes refers to an individual, the list itself is the property of the party that compiled it. The individual to whom the attributes apply may be ignorant of the list’s existence or of its contents.

In the sense of the internationally recognized definition [13], “biometrics” is specifically recognition of human bodies—the body serving as a reasonable proxy for a human individual. The process starts with an initial encounter, which is generally called “enrollment,” at which biological and behavioral characteristics sufficient for subsequent recognition are entered (stored) into a database for future comparisons. We must not infer that such enrollment necessitates the knowledge or cooperation of the individual enrolled or the collection of any information beyond the biometric characteristics. We hope, of course, that such biometric characteristics are stable enough to allow recognition of

the individual at future times and distinctive enough to be considered individuating (allowing a one-to-one correspondence) over some limited population. We will call this limited population the “population of interest”². In some biometric systems, these biometric characteristics are used as the label for the attribute record. But in other biometric systems, nonbiometric labels are assigned, with the biometric characteristics treated as attributes [14].

So the initial encounter with an individual, whether overt or covert, results in the creation of a record of the encounter. If biometric characteristics are collected, those characteristics might form the label for the record or might be attributes stored in the record with a different label (“Individual 1234”).

The simplest role of a biometric system might be to determine whether or not a previous encounter with the individual has occurred by searching existing records for biometric characteristics used as either labels or attributes. This role has considerable application, sometimes referred to as “clustering” or, particularly over a single audio recording in speaker recognition, as “diarization.” An expanded role of a biometric system would be to use the collected biometric characteristics as an identifier to link the newly encountered individual to records of details of previous encounters or to determine that no record exists. If the collected biometric characteristics are sufficient to find an identifier, such as a name, number, or simply the biometric characteristic itself, that can be used by others to link to their own record of additional attributes for an individual, we say that biometric “identification” has occurred. But as illustrated with the example of milk, the attributes in the linked record might be transient, incomplete, or even incorrect. Regardless of the faith we have in the correct recognition of the identifier (the label), our belief in any associated nonbiometric attributes will always be tentative.

Given this background, biometric recognition can be considered as the use of automated technology to apply a stable and distinctive biometric identifier to an individual previously encountered. The application of attributes based on that label is subsequent to finding the label and not a necessary part of the biometric

recognition process³. Identification is thus not an inherent part of the process of recognizing an individual. Identification occurs when attributes are sufficient to generate a label for an individual which is distinguishing over a limited population of interest and can be communicated to others. These attributes might be a name, number, detailed description, or the biometric characteristic itself.

As we have mentioned above, biometric characteristics might be used not as the identifier but as attributes in a record labeled by other means. The collected biometric attributes could be compared to those already existing within a record labeled with a nonbiometric identifier ("Individual 1234"). If a claim has been made that a particular labeled record does or does not have biometric attributes consistent with those collected, we can call this application "verification," that is, determining the truth of the claim to association of the individual with the label (the identifier). My claim of either association or nonassociation with the identifier "Individual 1234" could be verified by comparing my biometric characteristics to the biometric attributes in the labeled record.

To summarize, biometric recognition requires only acknowledgment that the biometric characteristics of an individual have been encountered before. Biometric identification requires recognition of an identifier pointing to a record containing sufficient information for individuation over a population of interest. Verification implies supporting or denying a claim of an individual's association with a record by comparing biometric attributes to those of the record⁴.

3 | Identity as "Same" and Identity as "Self": Idem and Ipse

It may seem odd that we have developed the concept of "identification" without recourse to discussion of "identity," which is the subject of this section. Dictionaries usually define "identification" as the action of attributing an identity to someone or something, so our approach in this paper differs significantly from common parlance⁵. Linguistically, "identity" expresses tautology. "It is what it is." The identity operator in mathematics tells us that $A = A$ or perhaps $A = B$, meaning that "A" and "B" are synonymous labels. That does not imply, however, that identity operators cannot reveal significant information. The statement "Robert Francis Prevost is Pope Leo XIV" reveals information not contained in either element of the tautology alone. The added information comes when we understand that the identity operator has simply equated identifiers, each pointing to different, perhaps multiple, attribute records. We seek in this section to deconfound the concept of "identity" from both identifiers and attributes.

Identity and identification both come from the Latin word *idem*, which literally means "the same"; identifying then means "to regard as the same." Different things cannot actually be the same, for to say that two things are identical is to say that in one sense they are two, but that in another sense they are one. For if they were really two, they would not really be identical. As Wittgenstein [15] famously wrote "to say of two things that they are identical is nonsense, and to say of one thing that it is identical with itself is to say nothing at all." Clearly if we are to

understand biometrics, we must find a more articulated meaning in this concept of "identity."

So far in this paper, we stopped short of considering either the attributes or the labeling identifiers applied to a recognized individual as their "identity." We, as humans, cannot be reduced to our transient, incomplete, or incorrect attributes as stored in a system linked to biometric recognition, nor can we be reduced to our labels, biometric or otherwise. Therefore, the concept of "personal identity" demands significant further explication.

The concept "personal identity" can be broken into two types: "identity as" (*idem/same*) and "identity of" (*ipse/self*) [16, 17]. We may consider ourselves as members of various groups, geographies, or professions, as in "My identity as a scientist." This is one approach to the concept of "*idem*," the Latin word meaning "same." With biometric technologies, however, the concept of "*idem*" is limited to observable biological and behavioral characteristics. As the number of observable biometric characteristics increases and their prevalence in the population decreases, the number of people similar to me decreases rapidly until ultimately, there is only one person in the population of interest who is the "same as" me. This further implies that the characteristics used for "*idem*" identity must be stable on the time scale over which recognition is to occur. If I⁶ can be recognized within the population of interest as previously encountered over some time interval and there are sufficient attributes to distinguish me from the rest of the individuals in that population, we say I have been biometrically "identified," meaning that a label based on biometric characteristics, which can be communicated and linked to other records, has been applied. This is biometric identity in the sense of *idem*: application of a sufficiently distinctive biometric-based label allowing linkage to records of attributes of only one person in the population of interest. It is in this sense that biometric technologies can "identify" an individual using observable attributes such as face, fingerprints, or iris pattern: narrowing down the membership group to a single body, which can be associated with attributes acquired in the previous encounters⁷. In the absence of a distinguishing label or information from the previous encounter, we can only say that the individual has been recognized⁸.

The other type of identity is that of "*ipse*," the Latin word meaning "self." This concept of identity is not that of sameness, but rather of difference from others. It is this concept of "identity" that makes me metaphysically unique and therefore "special," "one of a kind," "the real me." *Ipse*-identity is how I define myself and may involve personal labels and attributes that I currently associate with my existence. Although I may share some of these labeled differences with others, "*ipse*" does not imply sameness with anything and, unlike "*idem*," does not require stability in any time interval and is, in fact, generally changing across time as I move through various stages of life.

The attributes linked through "identification" of the "*idem*" identity may be closely related to the attributes in an "*ipse*" identity. If multiple systems based on the same "*idem*" identifiers—which in our case can be biometric characteristics—contain different linked attributes, it will be possible to link some aspects of "*ipse*" identity across applications. Biometric characteristics linked to my financial records could be used to link to my health care records, revealing my health status to my bank. Those

attributes might be significant components to my understanding of self. Thus, idem-identification might reveal aspects of my ipse-identity to others in ways that I cannot control.

In recent decades, some biometric systems have been developed to find idem membership with populations, allowing inferences about ipse-identity attributes considered entirely personal. There are some current automated systems claiming to allow classification of persons by gender [18, 19], ethnicity [20], age [21], and even sexual [22] or political [23] orientation. This idem-identity approach of automated systems potentially revealing details of my ipse-identity by connecting my concept of self as personal difference to groups with similar attributes has recently been referred to as “biometric analysis,” as opposed to “biometric recognition”⁹. This application clearly presents a risk for revealing aspects of ipse-identity that individuals might wish to remain confidential and therefore should be controlled. The focus of large-scale biometric systems, particularly when used by Western governments, however, has been on differentiating persons, not classifying them, with limitations increasingly being put into place regarding biometric analysis [24].

4 | Risks Inherent in Biometric Recognition

The widespread deployment of automated biometric systems, largely driven by AI, has enabled biometric analysis to scale across an increasing number of applications. Concurrently, the collection, linking, and reuse of large datasets have considerably increased the risk of reidentification—connecting an individual’s attributes across applications. Attribute records originating from heterogeneous sources can now be mined, merged, and repurposed, enabling persistent tracking and detailed social profiling. These developments raise concerns not only regarding individual privacy but also risks to “group privacy,” where the identification of categories or types of individuals can lead to discrimination or even group-targeted harm.

This trend is particularly evident in the domain of digital identity. As internet use evolved from passive consumption to active participation, individuals began to continuously contribute fragments of personal data to the digital environment. These fragments, whether shared voluntarily or extracted implicitly, accumulate into complex digital identities that often become more operationally relevant than the physical individual. The governance of digital identity has therefore become a central technical and regulatory challenge. In the EU, frameworks such as the General Data Protection Regulation (GDPR) [25] and the European Union’s Data Act [26] promote decentralized models of identity management. While decentralization can enhance user control, it also increases the number of attributes that can be linked across contexts, enabling the creation of ad hoc populations and subpopulations. This has given rise to a new risk: digital discrimination.

“Digital discrimination” is defined as systematic and unfair treatment based on individual or group characteristics. In the context of biometric systems, potential areas of concern include both direct and indirect discrimination. Direct discrimination occurs when individuals are treated unfairly based on characteristics such as race, ethnicity, religion, sex, or sexual orientation. In the context of biometric applications, this frequently translates

into risks to the principles of inclusion—elevated false rejection and false acceptance rates for specific demographic groups, including women and people of color.

These disparities typically stem from two sources: (1) acquisition procedures and sensors that are less accessible or less effective for certain users; (2) biased training data or algorithms that produce uneven error distributions across populations.

Indirect discrimination can be more subtle. It occurs when formally neutral criteria disproportionately disadvantage specific groups. In the context of biometric systems, this issue often arises due to opaque algorithmic processes, the internal logic of which is difficult to audit. For instance, enrollment failures or repeated false rejections may indirectly encode information about disability, illness, or physical characteristics. Individuals using wheelchairs, those with dwarfism, or those with facial injuries or medical dressings may be systematically misrecognized by facial biometric systems.

Additionally, biometric systems have the potential to facilitate the inference of sensitive attributes. Performance variations across attributes such as gender, age, ethnicity, or eye color can lead to the indirect reconstruction of protected characteristics from enrollment difficulties or recognition errors. Gender and sexual orientation are increasingly inferred through profiling techniques that combine biometric data with online behavior, social networks, and transaction histories. These inferences are frequently rooted in stereotypes and represent a subtle form of discrimination, labeling, and mislabeling users.

The tension and interconnection between *ipse*- and *idem*-identity find their formal and normative expression in the concept of dignity, which underpins modern human rights frameworks (e.g., the 1948 Universal Declaration of Human Rights and the EU Charter of Fundamental Rights) [27, 28]. Human dignity is grounded in two complementary principles: the uniqueness and autonomy of each individual, and their capacity to be recognized and identified. Only individuals who are socially and legally recognizable can effectively be subjects of rights; without recognition, rights cannot be enforced [29].

Historically, the loss of recognition has been closely associated with the loss of dignity [30]. In ancient Rome, when a citizen was reduced to slavery, the first deprivation was the loss of their name. The unnamed individual ceased to exist as a legal and political subject. In this context, *dignitas* referred to social standing and recognized worth. Since the eighteenth century, the concept has evolved to denote the intrinsic and equal value of every human being, independent of status. Yet this intrinsic value still presupposes recognizability within a social and legal order.

The extreme consequences of severing identity from recognition were tragically demonstrated during the Nazi extermination camps. As documented by Levi [31], prisoners underwent systematic processes of deidentification: physical stripping, loss of personal belongings, and the erasure of names. Individuals were reduced to numerical tattoos, which functioned as the sole identifiers within the camp system. These numbers operated as minimal attribute records, sufficient for administrative control but deliberately disconnected from personal history, social relations, and moral agency.

This double deprivation—of *ipse*-identity (selfhood, autonomy, and interiority) and *idem*-identity (continuity and social

recognizability)—enabled total domination. Levi's analysis makes explicit that survival requires more than biological persistence; it requires an identity that is recognized by others. Within the camp, dignity and identity became mutually dependent; the loss of one entailed the loss of the other. The resulting "spiritual death" preceded and facilitated physical destruction.

From the perspective of biometrics and identification systems, this historical example highlights a critical point: identification is never neutral. Even minimal identifiers can support radically different social outcomes depending on how attribute records are embedded in legal, ethical, and institutional frameworks. Recognition that strips individuals of *ipse*-identity while retaining only a functional *idem*-identifier represents a failure of dignity, not its protection.

This analysis underscores that modern biometric systems must be evaluated not only in terms of accuracy and efficiency but also in terms of how they preserve the link between identification, recognition, and human dignity. However, these core concerns over the struggle between *idem*- and *ipse*-identity go back to the earliest developments of Western civilization. In the remainder of the paper, we will be concerned primarily with how the struggle for control of both *idem*- and *ipse*-identity have deep roots in Western Civilization and how these roots impact our understanding of biometric technologies today.

5 | Recognition and the Sameness of Self at the Dawn of Western Civilization: The Stories of Abraham and Odysseus

The twin notions of identity as sameness and difference appear at the very origins of Western culture. In *Mimesis*, Erich Auerbach identifies two foundational narrative models: the story of Odysseus and that of Abraham [32–34]. Both narratives revolve around recognition and misrecognition, and both emerge in a historical context marked by mobility, early urbanization, and the need to identify individuals across space and time.

While Auerbach focused on contrasting modes of representation in Homer and the Bible, here we focus on a different aspect: both narratives articulate early forms of identity management. They deal with subjects who move across territories and communities and must be recognized, or must prove who they are, through signs, marks, and behaviors—what today we would call identifiers and attribute records.

This concern emerged with the rise of complex societies in the late Neolithic and early Bronze Age, when growing populations and stable settlements required mechanisms for recognizing insiders and outsiders [35, 36]. Early identification systems existed in both Greece and Rome. In Greece, *symbola*—broken objects whose matching parts verified identity—functioned as portable credentials. In Rome, the *tessera hospitalitatis* acted as a form of guest credential, granting controlled access to the city through personal endorsement [37]. These practices anticipate later identification systems by linking personal identity to material or symbolic tokens.

Within this context, the biblical story of Abraham [38] can be read as a narrative of identity transformation and verification. Abram, a nomadic king-shepherd, receives a divine command to

leave his land and later to take a new name—Abraham—signaling a change in identity. This change is marked physically through circumcision, a bodily inscription that functions as a persistent identifier. The mark is both individual and collective, tying Abraham's identity to a covenant and making it recognizable across generations.

Abraham's story also illustrates the distinction between *idem*-identity (sameness over time) and *ipse*-identity (selfhood and commitment). Despite changes in name, status, and circumstance, Abraham remains the same person, while his identity is progressively redefined through actions, obedience, and belief. Circumcision operates as a biometric-like marker, but its meaning depends on an underlying behavioral and moral commitment, culminating in the episode of the sacrifice of Isaac. By circumcision, Abraham had his *ipse*-identity inscribed on his flesh, his body "written" with the sign of covenant with God. Circumcision, however, was much more than a mark on the flesh; it was already a symbolic allusion to the sacrifice of Isaac. The fateful moment when Abraham raised the knife to his son was already foreshadowed by the moment of circumcision. This is a symbolic short circuit of meaning between the two events. Abraham is recognized by God as a faithful man because of both. God recognizes Abraham's identity (*idem*) through the circumcision, but the circumcision is the outward sign of something deeper (*ipse*), which is only revealed (it emerges) when Abraham obeys the command to sacrifice Isaac. Abraham's identity of self is then threefold: (1) it is a physical sign; (2) it is a behavior sign; (3) it is a deeper belief—an intellectual and emotional state—impervious to changes in name and bodily markings (identifiers). Identity here is not reducible to a physical mark; it is validated through action and intent.

The other archetypal narrative, the Odyssey [39], is the story of the progressive revelation of an incognito hero, Odysseus (Ulysses in Latin). The eminent medievalist and Anglist, Piero Boitani [40], counted at least 30 episodes of recognition in the narrative poem. Boitani argues that the Odyssey is the greatest summa of recognition practices in Western literature. Odysseus' long journey is structured around repeated failures and successes of identification: through physical traits, scars, objects, memories, and knowledge. These operate as multimodal identifiers, some bodily, others cognitive or relational.

The poem begins with Odysseus arriving as a refugee among the Phaeacians. When he hears a blind bard chanting a poem about the Trojan War, he cannot help but burst into tears, thus revealing information about both his *idem*- and *ipse*-identities. The hero tells how he wandered the sea for 10 long years as a punishment from the gods after blinding the cyclops Polyphemus.

Having landed on an island in search of food, Odysseus and his companions were captured by a cannibal half-human Cyclops, Polyphemus, who first asked Odysseus's name (identifier). The hero answered, "My name is nobody" ("I have no identifier"). In the end, having blinded the terrible giant with a wooden stake, he managed to escape with a few friends. Polyphemus screamed and begged the other Cyclops to avenge him. But when the other Cyclopes asked, "Who blinded you?" Polyphemus replied, "Nobody," leaving them bewildered and unable to act¹⁰. Odysseus' concealment of his name from Polyphemus illustrates the strategic denial of identity, while his eventual recognition by his

dog, his nurse Eurycleia, his wife Penelope, and his father Laertes demonstrates different mechanisms of verification. The scar on his leg functions as a biometric marker; shared memories and private knowledge act as behavioral or contextual attributes. The Odyssey describes not only most of the ways in which an individual can be recognized but also the range of meanings that recognition practices can take: (1) to demonstrate one's own idem-identity as well as to reveal a hidden ipse-identity; (2) to establish whether someone is really present as well as to evoke someone who is absent; (3) to remain unknown as well as to claim one's social role and dignity. The story demonstrates the situationally dependent conflicts between recognition and non-recognition and the linkages to identification.

Together, the stories of Abraham and Odysseus show that identity is not equivalent to recognition. Recognition requires linking observable attributes to an assumed or remembered identity. This linkage can fail, be delayed, or be intentionally manipulated. These narratives anticipate key issues in modern biometric systems: the distinction between identity and identifiers, the role of context, the multiplicity of attributes, and the dependence of recognition on trust and interpretation rather than on technology alone.

In this sense, ancient narratives already articulate core problems of identification systems: how identity persists through change, how it is authenticated, and how recognition depends on both physical markers and social meaning.

6 | Conclusions

Biometric characteristics can be used as identifiers or as personal attributes in a record, which can lead to identification. When used as identifiers, they can allow the linking of individuals to records and allow the linking of records of personal attributes. But even if the characteristics are completely unchanging over time, they cannot guarantee the accuracy or completeness of anything in the record—that record being generally curated by someone other than the individual to whom it pertains. Even highly accurate records can only supply hints as to an individual's ipse-identity of self.

The recognition of identifiers of individuals through stable biological and behavioral characteristics (biometrics) by government and commercial interests seems both reasonable and desirable in some situations, such as various types of access control and benefit issuance. By extension, nonrecognition of idem-identity, such as for government benefit enrollment also can be a reasonable application of biometrics. But increasing dissemination of biometric identifiers to more systems only invites linkages to multiple records with an increasing scope of personal attributes linked to ipse-identity, the identity of self. The threat to personal privacy arises when biometric identifiers begin to reveal connections between attributes and aspects of ipse-identity, particularly when biometric characteristics are used to link an individual to distinctive populations based on race, religion, gender, sexual orientation, and the like. There cannot always be a clear delineation between revelation of identifiers and ipse-identities, as the stories of Abraham and Odysseus teach us. As biometrics connects individuals with records of attributes, it can also connect records to records through a common characteristic, allowing the composite

attributes to be inferred to that individual. Composite records might contain information sensitive in one context but not another, and such information might be unstable and impermanent. Characterizations of biometric technology as answering the questions “Who am I?” or “Am I the person I claim to be?” wrongly imply a necessary connection between idem-identity and ipse-identity. Biometrics can hint at, but does not have the capacity of determining, our “real identity” in the ipse sense. It is the connection between ipse- and idem-identity that should be minimized by control over what information is linked to the biometric identifiers, as has been frequently suggested [14, 41]

Under many conditions, biometric systems have a legitimate place in society for associating identifiers, as pointers, to records of personal attributes, such as citizenship, immigration status, and social benefit eligibility. Biometric systems can determine that such records do or do not exist but cannot determine the current veracity of any of the attributes in those records. Biometrics cannot determine or assign individual concepts of “self.” Our “selves” are not who the biometric systems say they are. The biometrics community would be well advised to focus on idem-identity and avoid any implications of using technology to reveal ipse-identity. Statements that biometrics can verify “who I am” or determine “if I am who I claim to be” are both incorrect and counterproductive to the understanding of our field. We remain autonomous individuals regardless of what technologies are applied to our bodies.

Biometric technologies certainly carry risks to privacy, inclusion, and human dignity. Responding appropriately to the very legitimate personal and societal concerns over current technologies addressing the age-old problems of “personal identification” requires us to articulate the differences and intersections between recognition, identifiers, identification, and the two forms of identity—“ipse” and “idem.” In this paper, we have shown that the tension between revealing and not revealing personal identifiers, thus protecting, allowing, or promoting recognition and linkages to information about self, is a major theme within Western civilization. Therefore, we should be not at all surprised that these concerns, when not carefully considered, manifest themselves today as opposition to deployment of biometric technologies, even for very legitimate and positive reasons [42, 43]. By acknowledging and addressing these concerns head-on, we hope to forge a path forward toward appropriate and acceptable uses of biometrics.

Acknowledgments

The authors acknowledge very enlightening discussions with Prof. Charles D. Raab of the University of Edinburgh and Fellow of The Alan Turing Institute.

Funding

This article has been partly funded by the research project SOTERIA. SOTERIA has received funding from the European Union's Horizon 2020 research and innovation programme (Grant 10101834).

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Although the authors have been deeply involved historically in the development and analysis of biometric data, no datasets were generated or used directly in this study.

Endnotes

¹“Biometrics” is narrowly defined by the international standards community [13] as “automated recognition of individuals based on their biological and behavioral characteristics.”

²A “population of interest” consists of those individuals likely to be encountered in operation. So, for example, it is not necessary to show that a biometric measure is “unique” over all persons living and dead for a technology to be useful, only that it allows “individuation” within the population likely to be encountered.

³In Chinese public bathrooms, which dispense toilet paper only to persons not recognized as having recently received toilet paper, no attributes beyond the biometric identifier (the face image) and the fact of the encounter are ever collected. Beijing park dispenses loo roll using facial recognition—BBC News.

⁴The international standard for biometric vocabulary [13] defines biometric verification as the “process of confirming a *biometric claim* through *comparison*.”

⁵The study [13] defines 198 words in common usage in the field without using the term “identity” at all, other than two occurrences in clarifying footnotes.

⁶In this section, we choose to discuss the concept of identity more consistently in the first person to emphasize the very personal nature of this concept.

⁷In forensic applications, automated processes can be augmented by human intervention in the case of multiple potential labels being found in searches of a large database.

⁸Information linked to labels might be minimal, such as merely “this person previously encountered.” The previously noted public Chinese systems for dispensing toilet paper to persons previously not encountered is but one example.

⁹See, for instance, the U.S. National Institute of Standards and Technology webpage Face Technology Evaluations—FRTE/FATE | NIST. “Biometric analysis” has also been referred to as “soft biometrics,” which can be used as a technique for restricting a large-scale search to just part of the database.

¹⁰The other Cyclopes confused “no identifier” as being the identifier. Instances of this confusion in modern contexts continue. See What Happens When Your License Plate Says “NO PLATE?” | Snopes.com.

References

1. J. L. Wayman, “The Scientific Development of Biometrics Over the Last 40 Years”, in *The History of Information Security: A Comprehensive Handbook*, (Elsevier, eds. K. deLeeuw and J. A. Bergstra, (2007).
2. A. K. Jain, K. Nandakumar, and A. Ross, “50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities,” *Pattern Recognition Letters* 79 (2016): 80–105.
3. D. Wilson, “Australian Biometrics and Global Surveillance,” *International Criminal Justice Review* 17, no. 3 (2007): 207–219.
4. G. E. Hunter, “The Use of Technology to Invade Personal Privacy in the Interest of Collective Security: Does the End Justify the Means?” *Law Technology* 40, no. 1 (2007): 1.
5. P. Dixon, “A Failure to “Do No Harm”—India’s Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the US,” *Health and Technology* 7, no. 4 (2017): 539–567.
6. A. Thaker, “The New Oil: Aadhaar’s Mixing of Public Risk and Private Profit,” 2018, Caravan, 1 May (<https://www.caravanmagazine.in/reportage/aadhaar-mixing-public-risk-private-profit>).

7. A. Jain, R. Bolle, and S. Pankanti, *Introduction to Biometrics* (Springer US, 1996): 1–41.
8. A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, “An Identity-Authentication System Using Fingerprints,” *Proceedings of the IEEE* 85, no. 9 (1997): 1365–1388.
9. W. C. Shen and R. Khanna, “Scanning the Special Issue on Automated Biometrics,” *Proceedings of the IEEE* 85, no. 9: 1343–1346.
10. R. Hummel, et al., “Authentication Using Biometrics: How to Prove Who You Are,” in *STEPS: Science, Technology, Engineering & Policy Studies* 5, (2021).
11. M. C. Banville, “Am i who i Say i Am? the Illusion of Choice: Biometric Identification in Healthcare,” (2023).
12. A. Kind, “Biometrics and the Metaphysics of Personal Identity,” *IET Biometrics* 12, no. 3 (2023): 176–182.
13. ISO/IEC, “International Organization for Standardization, International Electrotechnical Commission, Information Technology – Vocabulary – Part: 37 Biometrics,” 2382-37 (2022).
14. Stephen T. Kent and Lynette I. Millett, Eds. “Who Goes There?: Authentication Through the Lens of Privacy,” (National Academies Press, 2003).
15. L. Wittgenstein, “Tractatus Logico-Philosophicus by Ludwig Wittgenstein,” *Journal of the History of Ideas* 59 (1922): 1–28.
16. P. Ricoeur, *Oneself as Another* (University of Chicago Press, 1992).
17. M. Hildebrandt, “European Criminal Law and European Identity,” *Criminal Law and Philosophy* 1, no. 1 (2007): 57–78.
18. X. Li, S. J. Maybank, S. Yan, D. Tao, and D. Xu, “Gait Components and Their Application to Gender Recognition,” *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 38, no. 2 (2008): 145–155.
19. W. Zhang, M. L. Smith, L. N. Smith, and A. Farooq, “Gender Recognition From Facial Images: Two or Three Dimensions?” *Journal of the Optical Society of America A* 33, no. 3 (2016): 333–344.
20. J. Leibold, “Surveillance in China’s Xinjiang Region: Ethnic Sorting, Coercion, and Inducement,” *Journal of Contemporary China* 29, no. 121 (2020): 46–60.
21. M. L. Ngan and P. J. Grother, “Face Recognition Vendor Test (frvt)-Performance of Automated Age Estimation Algorithms,” (2014).
22. Y. Wang and M. Kosinski, “Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation From Facial Images,” *Journal of Personality and Social Psychology* 114, no. 2 (2018): 246–257.
23. M. Kosinski, “Facial Recognition Technology Can Expose Political Orientation From Naturalistic Facial Images,” *Scientific Reports* 11, no. 1 (2021): 100.
24. U S, “Department of Homeland Security Directive 026-11, “Use of Face Recognition and Face Capture Technologies,” 2023, https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capture-technologies.pdf.
25. European Union, “General Data Privacy Regulation” Article 5.1-2 2016 gdpr.eu”.
26. OJL, “Regulation (EU) 2023/2854 of the European Parliament and the Council of 13 December 2023 on Harmonized Rules of Fair Access to and use of Data,” (2023).
27. J. Waldron, “Is Dignity the Foundation of Human Rights?” in *Philosophical Foundations of Human Rights, Philosophical Foundations of Law*, eds. S. Matthew Liao Rowan Cruft and Massimo Renzo, (2015).
28. G. Fletcher, “Human Dignity as a Constitutional Value,” *University of Western Ontario Law Review* 22 (1984): 178.

29. E. Mordini and M. Green, "Identity, Security, and Democracy: The Wider Social and Ethical Implications of Automated Systems for Human Identification," *NATO Science for Peace and Security Series* 49 (2023).
30. M. Rosen, *Dignity: Its History and Meaning* (Harvard University Press, 2012).
31. P. Levi, *If This Is a Man (Survival in Auschwitz, U.S.)* (The Orion Press, 1959, 1947).
32. G. Green, "Literary Criticism & the Structures of History, Erich Auerbach & Leo Spitzer," in *(No Title)*, (1982).
33. E. Auerbach, *Mimesis: The Representation of Reality in Western Literature* (Princeton University Press, 2003).
34. L. Morrissey, "Erich Auerbach (1892–1957) From 'Odysseus' Scar," *Mimesis* (1946; trans. 1953)." In *Debating the Canon: A Reader From Addison to Nafisi* (2005): 51–56.
35. A. W. Johnson and T. Earle, *Earle the Evolution of Human Societies* (Stanford University Press, 1987).
36. E. Mordini, "Biometrics, Identity, Recognition and the Private Sphere: Where We Are, Where We Go," in *User-Centric Privacy and Security in Biometrics*, (2017): 377–399.
37. C. Phillipson, *The International Law and Custom of Ancient Rome and Greece* (Macmillan and Co. Limited, 1911).
38. "Genesis 22:2".
39. Homer, *The Odyssey* (W.W. Norton, 2018).
40. P. Boitani, "Something Divine in Recognition," in *Recognition and Modes of Knowledge: Anagnorisis from Antiquity to Contemporary Theory*, (2013): 1–32.
41. Lynette I. Millett and Joseph N. Pato, Eds. "Biometric Recognition: Challenges and Opportunities," (2010).
42. A. Ioannou, I. Tussyadiah, and Y. Lu, "Privacy Concerns and Disclosure of Biometric and Behavioral Data for Travel," *International Journal of Information Management* 54 (2020): 102122.
43. I. Cooper and J. Yon, "Ethical Issues in Biometrics," *Science Insights* 30, no. 2 (2019): 63–69.