Partners Universal Innovative Research Publication (PUIRP)
Volume: 04 Issue: 04 | July - August 2026 | ISSN: 3048-586X | www.puirp.com

Behavioral Biometrics and Continuous Authentication: A Narrative Review of Technologies, Applications, and Governance Challenges

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India.

Abstract – Behavioral biometrics is one of the most impactful advancements in the field of digital identity and cybersecurity, making authentication not just a single point, but an ongoing process that is seamlessly integrated into everyday human activity. Behavioral biometrics, in contrast to physiological biometrics, captures the dynamic behavior of how people type, move, swipe, walk and interact with digital systems. This article aims to give a detailed awareness oriented overview of technology, its scientific basis, the main modalities and technical architecture, in an accessible way. It explores why technology is so quickly being adopted, such as the shortcomings of passwords, the increase in identity theft and the rise of digital life on the go. The benefits and impact on countries, companies and individuals are discussed, as well as the economic drivers of the field. The same attention is paid to the risks, which include privacy erosion, consent challenges, demographic bias, and the historical lack of attention to governance frameworks in line with technological deployment. The article highlights some of the errors that future adopters should avoid and identifies remaining research gaps that need to be filled, given the lessons learned from past regulatory failures. To give readers of all stripes balanced, fact-filled knowledge of a technology that is watching us all the time, everywhere, and anywhere.

Keywords: Behavioral biometrics, Continuous authentication, Keystroke dynamics, Fraud detection, Digital identity, Data privacy, Risk-based authentication, Cybersecurity governance.

1. INTRODUCTION

All people have a secret stamp. It's not ink, or even a fingerprint or an iris pattern. It's found rather in the beat of typing, the swipe of a thumb across a screen, the slight shake of a hand that holds a phone, the pace of a walk, the delay of a cursor before clicking. These patterns take years to develop as a neuromuscular habit and cognitive development and are quite unique and hard to replicate. The science of measuring and using them is called behavioural biometrics, and it's subtly changing the way that the modern world builds trust between people and machines.

Throughout the digital era, the two most common methods for identity verification are based on what people know e.g., password, personal questions or on what they have e.g., card, phone. Both methods have a critical flaw in that they only validate a credential, not an individual. When a criminal gets a stolen password, it is as good as if the victim had the same password. Even the physiological biometrics like fingerprint or face recognition, only establish identity at a particular point in time. The system stops monitoring when the door is opened. Fraudsters have discovered how to take advantage of this very vulnerability they have been able to hijack sessions after a user has logged in, to force victims to approve transactions or to use automated software that simulates a human user on a large scale.

Behavioral biometrics aims to overcome this vulnerability by shifting the question to, who is using this system right now, and are they acting like themselves. It moves authentication from a gate to a companion that watches at all times, and says nothing, and does nothing, just watches, and doesn't ask the person to

stop and pose and put their finger to a sensor. This method has quickly progressed from research labs to banking systems, government portals, work place systems and consumer devices. It is used by financial institutions to identify in-progress account takeover. Public agencies delve into it in order to safeguard digital services from organized fraud. It is used by employers to ensure working remotely. It has established its market footprint in a similar fashion as the losses from cybercrime have increased and users' impatience with burdensome security measures has also increased.

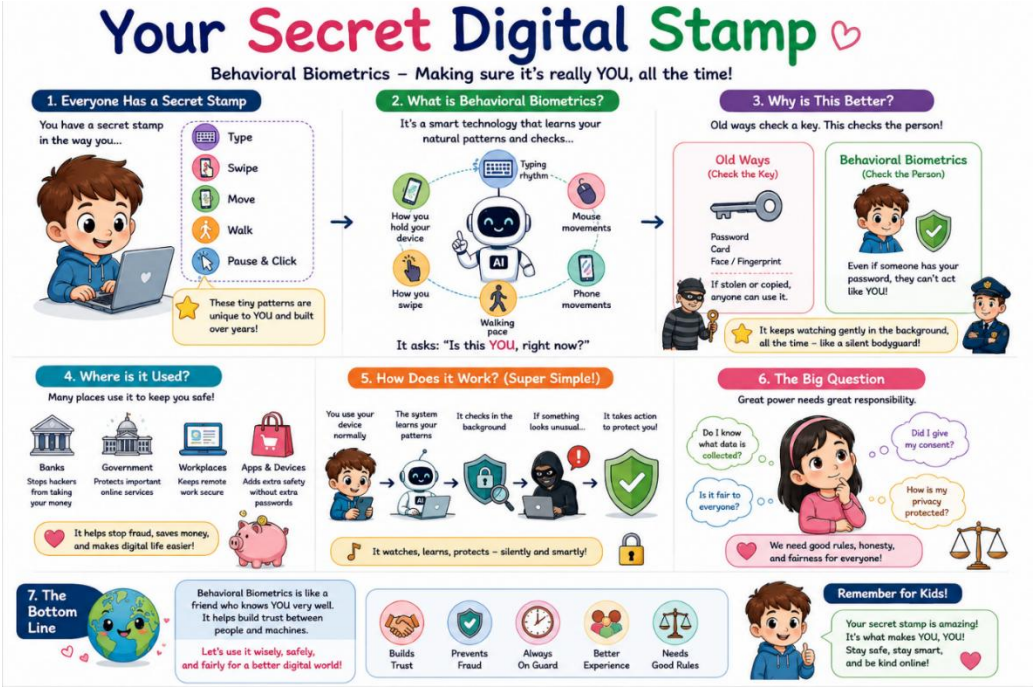

Fig –1: Understanding Behavioral Biometrics

However, these are the same attributes that make behavioral biometrics strong that make it weak. The technology that monitors the behaviour of people constantly and invisibly, brings up a lot of questions in terms of consent, surveillance, fairness and acceptable monitoring. History has many sobering lessons societies have often embraced transformative technologies before the law and ethics necessary to govern them have been developed and the costs of this delay have not been distributed equally among populations. The article provides an in-depth, balanced analysis of behavioral biometrics for a wide audience policymakers, business leaders, students and consumers of digital services. It provides explanations for the nature and function of the technology, its reasons for its proliferation, the benefits it brings to countries, companies and people, the economic drivers behind it and the risks and governance lessons that need to be learned. The goal is not to promote it, or to alarm, but to make people aware, and a technology that watches all of us should be understood by all of us.

2. OBJECTIVES OF THE ARTICLE

This article has six related aims.

1. First, it aims to provide explanations in non-specialist language of the scientific and technical underpinnings of behavioral biometrics, including the key modalities and the machine learning algorithms used to transform human behavior to a trust decision.

2. Second, it seeks to explain why this technology has come about now, in the context of the well-documented inadequacies of password-based security, and the increasing sophistication of digital fraud.
3. Third, it examines the benefits and impact of the technology at three levels of society: national governments public institutions, enterprises corporate organisations and individual citizens individual consumers.
4. Fourth, it explores the economic and business aspects of the field, understanding the rationale behind investment and adoption in a market, without focusing on any particular business entity.
5. Fifth, it discusses the risks, ethical issues and governance challenges the technology poses, taking a neutral view of past regulatory failures in order to learn from them for the benefit of future decision makers.
6. Finally, it maps out the research and knowledge deficits for researchers, regulators and practitioners. In all cases, the article is factual, well balanced and impartial, refraining from any bias towards or against countries, communities or institutions and from any bias in the presentation of uncertainty where the evidence is still unclear.

3. METHODOLOGY

The approach used in this article is that of a narrative, integrative review, which is appropriate for synthesizing knowledge in a rapidly changing, multidisciplinary field in order to communicate to a general and professional audience. The analysis is based on publicly available and verifiable sources, such as peer-reviewed academic literature on continuous authentication and behavioral biometric systems, mostly published since 2017, technical standards and guidance documents from the international standards bodies and professional biometrics associations, government and regulatory publications on biometric data protection in various jurisdictions, and reputable industry research on fraud trends and market development which is cited generically without naming any commercial vendors.

Sources were chosen based on three criteria being up-to-date, including content up to 2025-2026 to ensure that the state of the field is represented; credibility, favouring peer-reviewed research, official regulatory documents and trusted professional organisations over promotional content and relevance, including material that is relevant to the topic of behavioural rather than purely physiological biometrics. In the event that quantitative claims are made, they are presented in the most conservative manner and as findings rather than fact, given the variability in studies in this area. The synthesis is thematic and does not follow the chronological order of the documents, but rather from technical bases to societal applications, risks and governance. There were no original experiments, but the integration, contextualization, and translation to public awareness of specialist knowledge is the contribution of this article. The potential for publication bias in the underlying literature and the quickening pace of change in the field are recognised in research gaps discussion.

4. THE SCIENCE BEHIND BEHAVIORAL BIOMETRICS WHY BEHAVIOR IS A SIGNATURE

To appreciate the effectiveness of behavioral biometrics, let's take a look at a simple experiment. Have 2 people type the same sentence using the same keyboard. The words will be the same, but so will not be the performances. One person keeps a few keys down a few milliseconds longer, another seems to hesitate

before hitting the period, or the other person types pairs of common letters at a very fast rate that he or she has memorized over the years. These differences are not due to random noise. They reflect underlying, highly personal, neuromuscular and cognitive processes, influenced by physiology, education, habit, language background and even personality.

The principle of behavioral biometrics is based on a well-established fact of psychology and motor control studies complex learned behaviors are highly automatized and highly individual. The gait pattern of a walking person is the result of the coordinated action of hundreds of muscles, and has a cadence, stride length and body sway that is characteristic of the individual. The path, acceleration and correction of a computer mouse movement towards a button is a reflection of the motor planning of the person. The angle, grip pressure and micro-movements of a person's hand when holding a smartphone is a constant pattern over time. The behaviours are repeated thousands of times and the person would find it difficult to change their behaviour if they were asked to and an impostor would find it difficult to replicate the behaviour even if they were shown it.

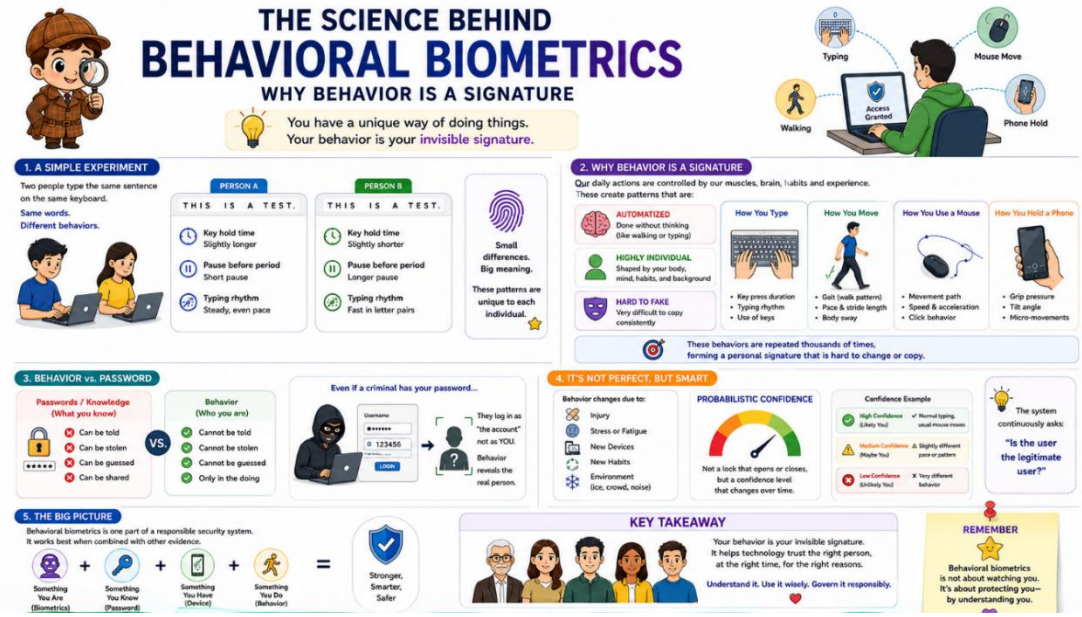

Fig -2: The Science Behin Behavioral Biometrics

It is this that sets behavioral biometrics apart from knowledge-based security. A password can be told, stolen or guessed as it is information that can be separated from the person. You can't pass on a behavior pattern, it's only in the doing. When a criminal logs in with a victim's password and victim's one-time code, he or she logs in as him or her not as the victim. The literature of continuous authentication has consistently shown that using more than one behaviour will make this distinction more reliable and less prone to false alarms as whilst one behaviour might be different due to mood, fatigue or circumstance, a combination of behaviours will be recognisable as each individual's.

Honestly, it is crucial to inform about the limits. Behavioral patterns are not definite, but probabilistic. They fade as you grow, get injured, experience stress, new devices and new habits. A person with a broken finger or walking on ice, is not the same as when they are not broken or on ice. That's why behavioral biometrics isn't so much a lock that opens or closes, as it is a constantly changing level of confidence, a constantly evolving answer to the question, Is the user the legitimate user. This probabilistic nature influences the

design of the technology, how it is deployed, and how it is governed and is what makes behavioral signals one of several sources of evidence for responsible systems.

5. THE PRINCIPAL MODALITIES READING THE MANY LANGUAGES OF HUMAN BEHAVIOR

Behavioral biometrics is not one technique, but a set of measurement techniques each of which is sensitive to a different channel of human activity. These modalities help the public to see the range of the technology, and the range of data it impacts.

The oldest and most investigated modality is keystroke dynamics, which has been studied for decades, since telegraph operators were found to be identifiable based on their transmission rhythm. Current systems record dwell time how long each key is being pressed and flight time how long it takes to let go of one key and press another, as well as typing speed, rhythm, error and correction rates, and if the hardware can support it pressure. A typing profile is created from these measurements that is distinctive enough to be used to identify individuals with a degree of significance, especially when the text sample is longer.

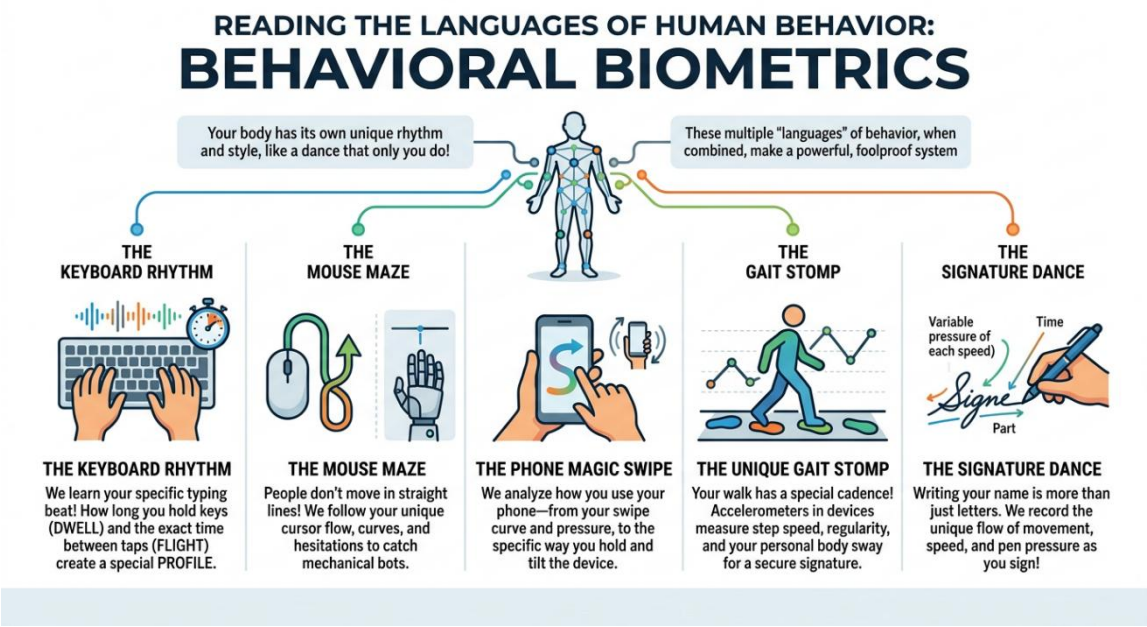

Fig -3: Reading the Languages of Human Behavior

A second rich channel on desktop systems is the way that mice and cursors behave. A motor signature is the velocity and the curvature of pointer movements, the approach and click strategy to targets, scrolling habits, drag patterns and hesitation points. This modality has been particularly useful in discriminating between human users and automated scripts, which traditionally move the mouse pointer in a very mechanical manner or in straight lines.

In the mobile world, gestures on the touchscreen are the predominant form of interaction. Systems monitor swipe gestures, how curved they are, how hard the tap is, how much area is being touched, how fast the scroll is, pinch and zoom gestures, and the duration of the gesture. Not far off is device handling the accelerometers and gyroscopes in today's phones can tell how a device is tilted, how steady the hand is, the preferred direction for holding the device, and the micro-tremors of a specific hand.

The same motion sensors are used for gait analysis to describe the gait, such as step frequency, stride regularity and body sway. It has been investigated for use in wearable devices for authentication as well as health monitoring, where gait changes may be a sign of medical issues, and has obvious ethical implications.

Other modalities include signature dynamics, which records the movement, pressure and time spent on a handwritten signature, voice cadence and speech rhythm not physiological voiceprints, and navigation behavior, which includes how a user navigates an application, the order of screens visited, familiarity or unfamiliarity with menus, and the speed of a session. Navigation analysis is especially useful in spotting criminals who log on to a stolen account, as a fraudster would use an account interface differently than a longtime account holder, or be more at ease doing things that a regular customer would not do, such as changing contact information and adding new payees in quick succession. The most powerful systems are those which involve multiple modalities, as behavior is multi-lingual and an impostor seldom speaks all of the languages.

6. HOW TECHNOLOGY WORKS FROM RAW SIGNALS TO TRUST DECISIONS

But behind the invisible workings of behavioural biometrics is a highly structured technical pipeline and knowing this goes a long way to demystifying the technology. This can be broken down into 7 stages, which are ongoing and are mostly real-time.

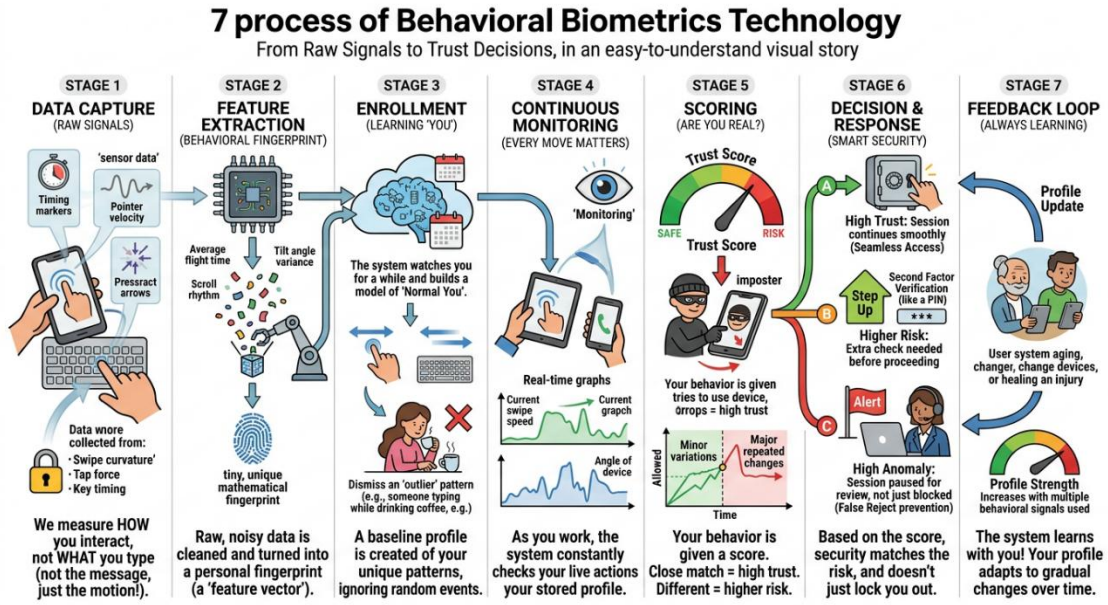

Fig -4: 7 Process of Behavioral Biometrics Technology

The initial step is data capturing. Software captures raw traces of the interaction as the user interacts with a device or application: when the user presses a key, when the key is released, where the pointer or finger is moved and how fast, how much pressure is applied, and streams from motion sensors. Most important, the well-designed systems do not measure the content of the behavior, but rather the mechanics of the behavior. They measure how a password is typed, not what the password is, and how a message is composed, not what the message says. This is a distinction that is of immense importance when it comes to privacy and should be the first question that the public asks with regard to any deployment.

The second stage is the feature extraction. Raw sensor streams are very noisy and voluminous, and the system calculates summary features such as average dwell times for specific keys, curvature statistics of the swipes or gait frequency components. The features are combined into mathematical representations, known as feature vectors, that serve as a short fingerprints of the behaviors.

The third step is the enrollment creation of profile. Machine learning models are trained over a number of sessions to understand what is normal for that particular user, so a reference template is created that accounts for the patterns that occur consistently, and ignores outliers e.g. the day the user types one handed while holding a cup of coffee.

The fourth and fifth stages are used in conjunction in normal use, Continuous monitoring and scoring. The current behavior is compared to the stored profile and a similarity risk score is calculated continuously. There are minor variations allowed as human behavior is variable, but major and or repeated variations increase the risk score.

Decision and response is the sixth stage and it is the most important stage in which design philosophy is important. A high confidence match means that the session can run smoothly. A high risk score can result in a higher level challenge e.g. second verification factor and a high anomaly score may result in the session being paused or put under human investigation. Responsible systems will not automatically block accounts in extreme cases, but will pass on the ambiguity to further verification, not denial, since it is bad for legitimate users if they are denied based on a false accusation of fraud.

The seventh stage is called the feedback loop. Profiles are continually changed over time as the system adapts to the user's gradual changes, due to age, new device or healed injury. This adaptive learning is the key to keeping false rejection rates low over the years of use, and recent studies have shown that combining several behavioral signals in such adaptive architectures can actually enhance the robustness. The beauty of the entire pipeline is that the user does not know it is there, and security is not intrusive.

7. WHY NOW THE FAILURES THAT MADE BEHAVIORAL BIOMETRICS NECESSARY

Technologies hardly ever rise to the level of being used on their own merits, but because the previous arrangements are failing. Behavioral biometrics' momentum stems from the cumulative failures of the previous generation of security models, and the reasons behind the failures are why the technology is not just filling in security gaps, but is changing the practice.

The first failure will be the password. Over the years, it has been proven that the human being is not able to carry the responsibility of secret-keeping that password security places on him or her. Users share passwords between services, select easy to remember and guessable passwords and hand over passwords to seemingly legitimate phishing emails. Vast collections of stolen credentials are floating around in criminal networks, where automated attacks may be conducted by attempting to log on to thousands of services with stolen username password combinations. If successful, the attacker is to the system as if they were the legitimate user since the system only verified the credential.

The second failure is more subtle, it is the degradation of multi-factor authentication as a full solution. But, one-time codes and other factors made the job of attacking more expensive. Criminals adapted by intercepting codes, by taking over the phone numbers that receive codes and most of all by social engineering, where the victims are manipulated into approving authentications or making transactions themselves. In these situations of coercion and manipulation, all traditional checks are passed, since the

real user is really there, but his or her hesitation, guidance, abnormal rhythm and navigation indicate something is amiss. This type of fraud has become one of the most harmful categories of financial crime globally, and is one of the few types of fraud that can be detected by behavioral biometrics.

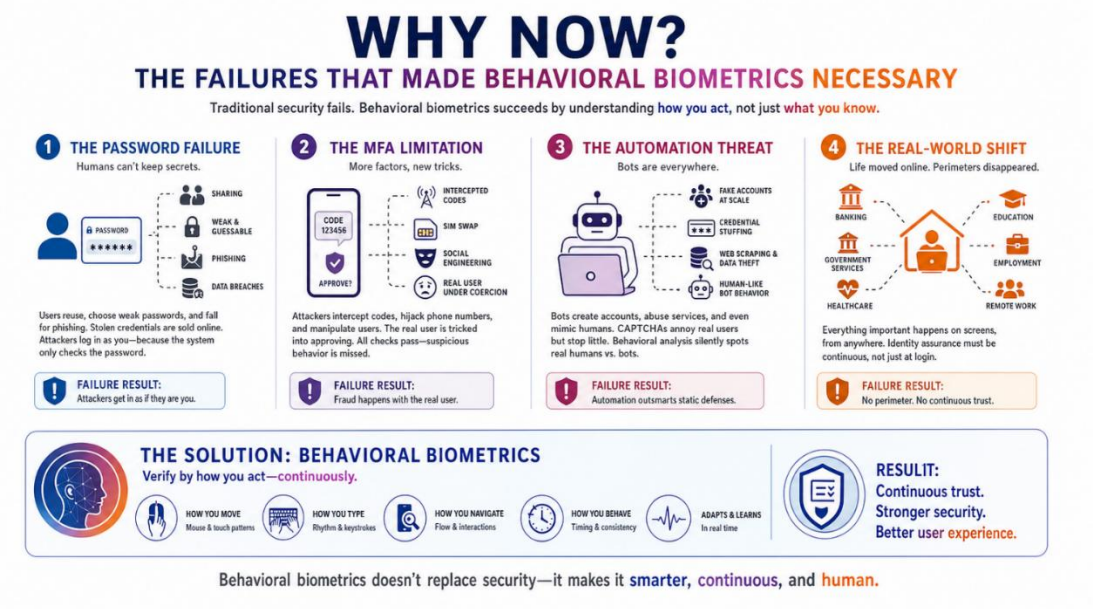

Fig -5: The Failures That Made Behavioral Biometrics Necessary

The third failure is with regard to automation. Today's Web is a battleground between people and software agents. Automated software programs generate fake accounts in bulk, steal and exploit services, and are increasingly able to mimic a human interaction. Puzzles that were once used to distinguish people from machines have evolved into a nuisance for real users, and a barely hindrance to advanced automation. Behavioral analysis is an alternative approach which does not require the user to do anything but identify organic human motor behaviour from synthetic interaction in a quiet way.

The fourth is life itself is changing. Banking, government services, healthcare, education and employment have all shifted to the virtual realm, and remote working has blown workforces out from the once secure boundaries. If the branch office, the government counter and the workplace are all a screen, then identity assurance must be a screen as well, but always and not just for a moment. Behavioral biometrics emerged as a solution to address just this gap: Vigilance for a world that is digital, that has long sessions, that starts with login and goes beyond.

8. CONTINUOUS AUTHENTICATION FROM A LOCKED DOOR TO A WATCHFUL COMPANION

The most fundamental change of perspective that behavioral biometrics entails is the transition from point-in-time verification to continuous authentication and it's important to explain this change, as it alters the grammar of digital security. Traditional security is like a locked door. Once the identity is verified, at entry, everything that happens after that is trusted at that point in time. The model is that anyone who passed the check is the person acting for the session. In many real-life situations this is not true. If you leave your device unlocked in a public area, it may be used by a stranger. A remote session can be compromised following login, using technical methods. Once the criminal is in, he has free reign with the credentials he stole and is able to beat secondary checks. A victim is manipulated by a fraudster over the phone and

authenticates perfectly and then, step by step, transfers his or her savings to a criminal. In all of these instances the locked door model has already said "yes" and there is no way to back down.

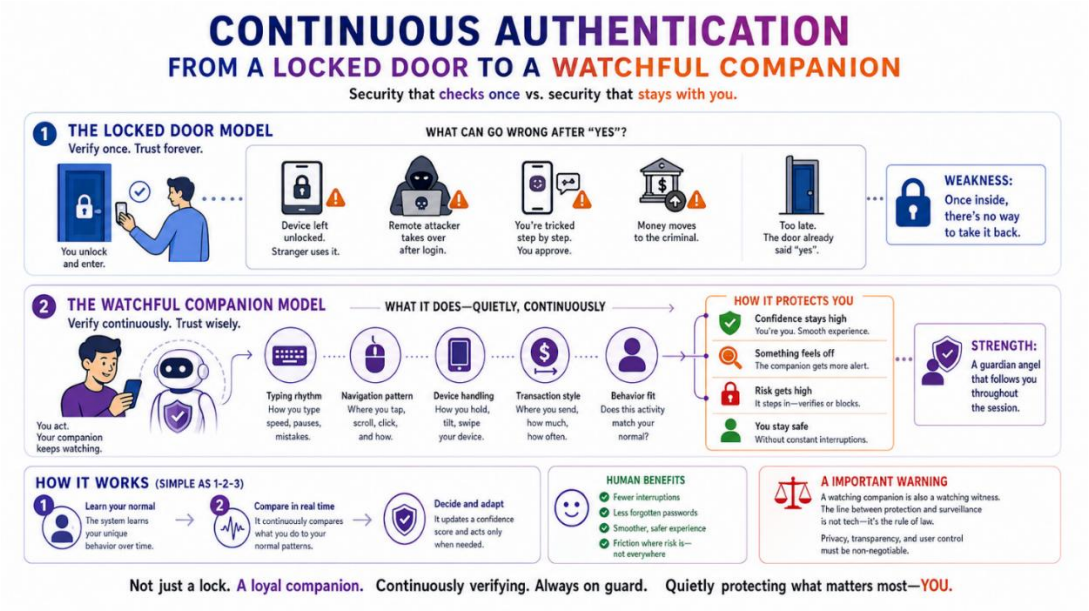

Fig -6: Continuous Authentication

Continuous Authentication is like the locked door but with a watchful companion. The system repeatedly, quietly and probabilistically asks, during the session, if the current behavior is still the same as the enrolled user behaving normally. A continuously updated confidence estimate is based on the typing rhythm, the navigation pattern, the way the device is handled, and the way the transactions are done. When a phone is used by multiple users during a session, the touch behavior of the new user deviates from the profile in a few moments. The interaction mechanics are completely different if a remote attacker takes control. When a true user is coerced or instructed, there are many clues, such as hesitation, unusual pauses, which would indicate listening to instructions, navigation to functions the user does not touch, and transaction patterns the user has not been involved with.

While the security value of this approach is easy to understand, so is its human value. With continuous authentication, there can be a rebalancing of friction. The system does not have to challenge the user repeatedly with codes and challenge during low-risk activities since it is always confident of the user's identity. Friction can be focused where there is risk, not spread to every user, every time they do an action. For the average consumer, it translates to less interruptions, less forgotten passwords and an online experience that isn't marred by security. Recent research has fittingly termed this paradigm a guardian angel one that is not stationed at the door, but rather one that follows the user around during the session. The companion metaphor also, however, has a warning. A watching companion is also, a watching witness, and the distinction between watching and surveillance is not a technological one, but a rule of law one. This tension is echoed throughout this article, and should be at the heart of any honest public debate on the field.

9. TRANSFORMATION FOR NATIONS AND GOVERNMENTS DIGITAL TRUST AS PUBLIC INFRASTRUCTURE

Behavioral biometrics comes at a time when digital identity is public infrastructure, just as vital as roads and power grids, for national governments. All regions have digitalized tax administration, social benefits, health services, licensing and civic participation. The savings are significant, but the risk is high a government website with millions of citizens using it is a juicy target for organized fraud and public dollars stolen through ID theft are ultimately lost by taxpayers and the vulnerable individuals benefit services are designed to protect.

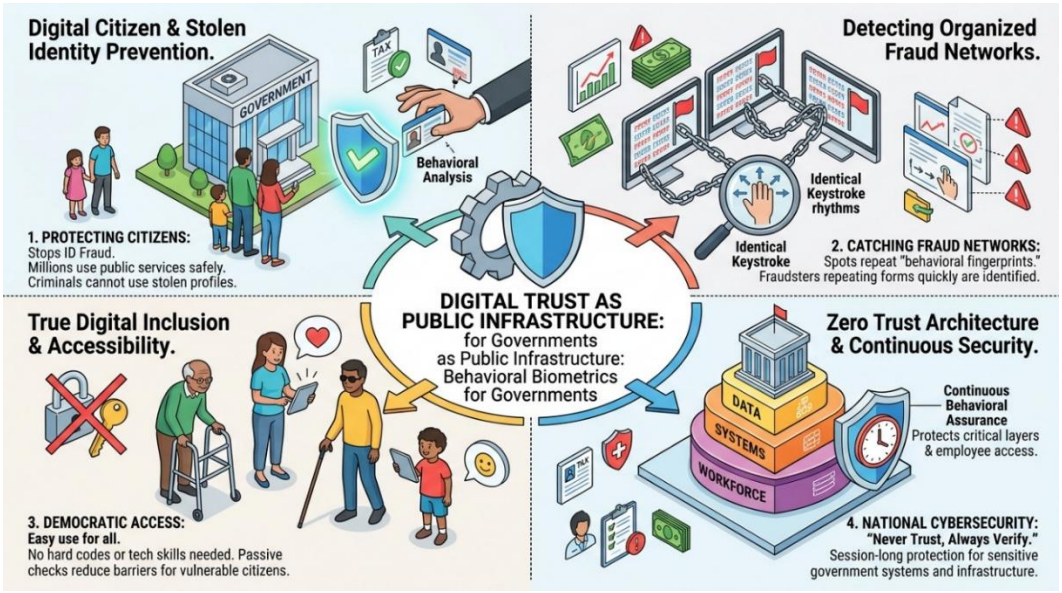

Fig -7: Digital Trust As Public Infrastructure

Governments have a number of unique capabilities with behavioral biometrics. Continuous behavioral analysis can be used in fraud prevention to identify organized abuse of benefit and relief programs, in which criminal groups file fraudulent claims on a large scale, using stolen identities. The behavioural fingerprint of such operations such as when the same form is practiced and rushed through by several supposedly unrelated claimants, or when the same pattern is repeated across several claimants can be measured and is clearly different from the behaviour of a genuine citizen seeing a form for the first time. Some governments have said that they have been investing in tooling for the detection of large-scale identity fraud and have changed their regulation accordingly, viewing identity fraud as a matter of national economic security.

The technology has an underappreciated democratic element in terms of accessibility to services. Traditional strong authentication can actually be more of a barrier for precisely the citizens who need public services those who have difficulty with codes or applications those who are illiterate or have limited digital literacy, and those who do not have the documents and or devices that other forms of authentication assume. Passive behavioural verification, in which the user does not have to do anything, can reduce such obstacles, without compromising assurance, and allows for true digital inclusion, rather than choosing between security and access. Continuous authentication is in line with zero-trust architectural principles, which have been embraced by many national cybersecurity strategies, where no session is trusted simply because it started off with good intentions. Session-long behavioral assurance is an added layer of protection that's useful in applications such as protecting government workforces, critical infrastructure operators and sensitive systems from insider misuse and credential-based intrusion.

But the government environment is where the misuses are most at risk as well. This is because if a state can passively verify a citizen's identity, without the citizen's knowledge, then a state can passively monitor a citizen's identity, without the citizen's knowledge. The distinctions are all in the purpose limitation, legal protections, independent oversight and transparency. The governmental tendency to re-purpose identity infrastructure is a recurring theme in history, and that is why international professional organizations in the biometrics space have expressed principles, such as proportionality, informed consent and strict purpose limitation. Countries with robust rule-of-law regimes that use behavioral biometrics can expect to be both secure and trusted by the public, and countries that use behavioral biometrics without robust rule of law regimes risk turning a security technology into a tool of control and the best defense against that is public awareness.

10. TRANSFORMATION FOR ENTERPRISES AND CORPORATIONS SECURITY THAT CUSTOMERS CANNOT FEEL

Behavioral biometrics has been solving a problem that has plagued the last decade of commerce for enterprises, and particularly in the banking and insurance sectors, as well as in retail and any organization with a digital scale, security and customer experience are at odds with each other. Each verification step further measurably deters fraud and each verification step further measurably deters customers. The cost of abandoned transactions, failed logins and support calls for locked accounts are on par with the cost of fraud losses. For enterprises, it has always been a matter of making a decision on this painful trade-off curve. Behavioral biometrics modifies the shape of the curve.

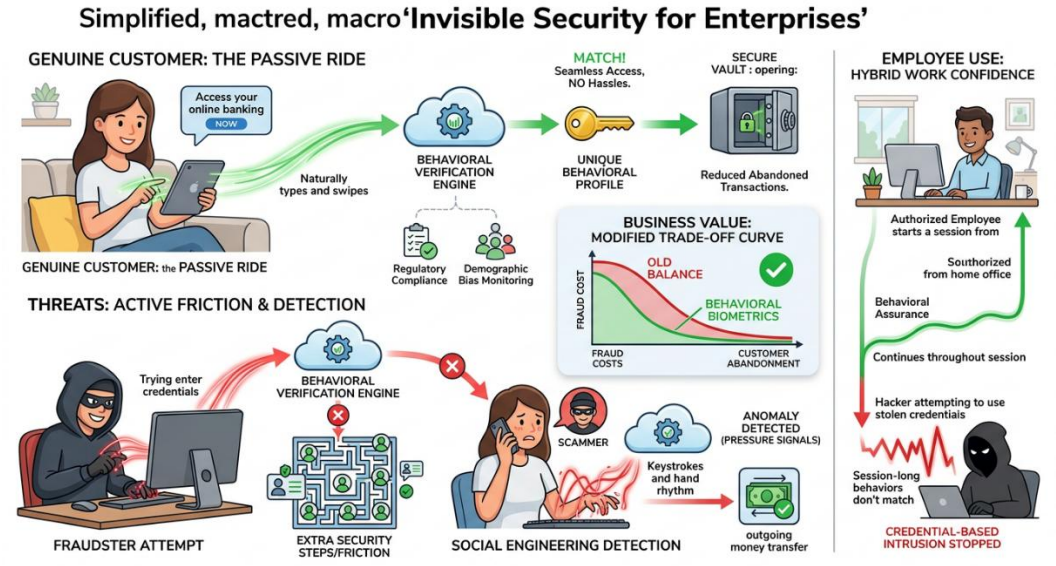

Fig -8: Invisible Security for Enterprises

Behavioral Verification is passive and therefore does not add steps but only adds assurance. A customer that comes back with typing, touch and navigation that are consistent with their profile can be given a nice ride with fewer hassles; the once in a while session that doesn't fit the profile can be given extra attention. This means that fraudsters will have to deal with increased friction while genuine customers will have less friction, as security effort is allocated based on evidence. In fraud operations, this means fewer false alarms requiring manual investigation, quicker fraud detection while the fraud is still in progress not after the funds

have been moved, and a materially improved ability to detect manipulation based fraud, in which the legitimate customer is tricked into transacting, a type of fraud to which traditional controls are structurally blind.

But there are also security threats to enterprises when it comes to their employees, which behavioral biometrics can help with. The physical boundaries have been broken down with remote and hybrid working, where an employee's session can start anywhere, on networks that are not in the employer's control. Continuous behavioral assurance will give the employee continuous confidence that the person using his or her privileged session is the authorized employee, thereby preventing external intrusion by using stolen staff credentials and certain types of internal misuse, such as sharing credentials. For regulated sectors, the technology also helps fulfill regulatory requirements related to customer authentication, fraud monitoring and transaction security that have been increasingly tightened by regulators in many jurisdictions.

There are also good costs and obligations on the enterprise side of the ledger. Implementing behavioral biometrics comes with an investment in the data infrastructure, data model governance, and expertise. It generates new types of sensitive information, the protection of which is not only an ethical and increasingly a legal obligation, as more and more jurisdictions consider biometric data as sensitive personal data that needs to be protected and consented to. It requires organizations to keep an eye on their systems to ensure that there is no demographic bias, and to offer a humane remedy for customers who are mis flagged. The companies that will reap the greatest long-term benefits from this technology are those that don't see it as a bolt on fraud solution, but as a tool for establishing a trust relationship with customers, used transparently, tightly controlled and with full disclosure. Once carelessly industrialized, trust is hard to come by.

11. TRANSFORMATION FOR INDIVIDUALS INVISIBLE PROTECTION IN EVERYDAY DIGITAL LIFE

The introduction of behavioral biometrics for the individual is largely unnoticeable, a good thing, but also the reason why it is so important to make people aware of it. It is important to describe in detail, and in terms of everyday life, what the technology does for an ordinary person the benefits and the concerns are both concrete.

Let's look at an individual who is making a bank transaction on a Tuesday evening. As they swipe their balance and pay a utility bill, they unconsciously confirm their touch pressure, swipe curvature and navigation rhythm to years of their own history, all while using the app on their phone. They are not required to do anything. Three weeks later, with the same account, the same password and the same verification code, but different: the device is held at a different angle, the navigation takes you straight to the function for adding a new payee, the typing rhythm is that of someone else. The session is put on hold and the real customer is notified before the transfer of his savings. The person might never come to know how close he or she came to losing it. This invisible rescue is multiplied by millions of users, and is the individual dividend of the technology.

The advantages are not just in terms of fraud prevention. Behavioral biometrics eliminates the daily burden that security adds to everyday life the need to re-enter codes, lockout rates and waiting at the checkout counter while an authentication fails. Passive protection is particularly useful for elderly users and those with cognitive impairment, who are more likely to be the victim of manipulation fraud and who are more likely to be overwhelmed by complicated security measures: it protects those who are least likely to be able

to protect themselves without requiring technical expertise from them. There is a protective aspect against coercion as well systems that detect behavioral cues of a user being coerced can put in a pause, warning or human touch at the opportune moment.

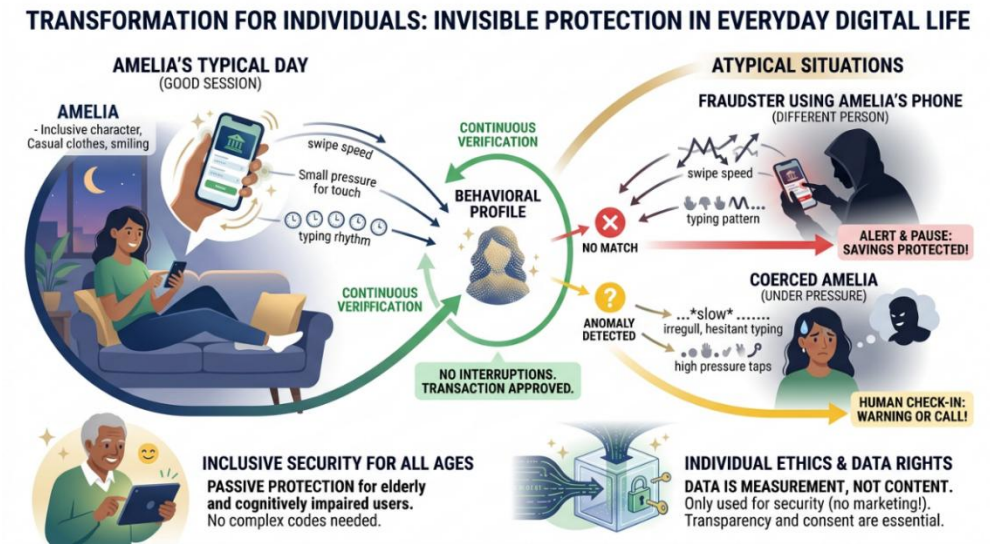

Fig -9: Invisible Protection in Everyday Digital Life

But the individual should also be aware of what he or she can expect of this technology. They should know that when data about their behaviour is collected it is for a purpose and be told this in clear terms. They should be aware that the data is a measurement of the mechanics of behaviour and not of the content of their communication. They should be aware that behavioural profiles are only used for security purposes and not used for marketing, profiling or evaluation without a specific agreement. They should be prepared for a humane method of correction, since a stroke victim or the man with the hurt hand will act differently and should not be locked out of his or her life. An informed public that poses these questions regularly is the most powerful element driving the industry towards its best practices and not the most expedient practices.

12. THE ECONOMY AND BUSINESS BEHIND TECHNOLOGY FOLLOWING THE MONEY

Any true story about a game changer technology must start with the economic force that is behind it, and there is clear economic logic behind behavioral biometrics the skyrocketing and increasing expense of digital fraud. When direct losses and remediation and downstream losses are considered, the losses from online fraud, account takeover, payment scams and identity crime are estimated to be hundreds of billions of dollars a year around the globe. Each percentage point of that loss avoided is a huge value and organizations willingly pay for technologies that can prove to help them avoid that loss. This is the basic business model for the behavioral biometrics business: Selling loss prevention, and loss prevention is a growth industry in a world of increased losses.

Year-over-year projections for behavioral biometrics have been solid double digits, across the industry, from the low billions to the many multiples of that amount, through the 2nd half of this decade. While the figures may differ depending on the source and the accuracy of the number is not as important as the direction it represents, the direction is clear and the drivers are structural fraud is becoming more sophisticated, regulation is becoming stricter in financial services in many jurisdictions regarding the

authentication of customers, volumes of digital transactions continue to rise and the cost of the customer experience of traditional security is an increasing driver for consideration of passive security.

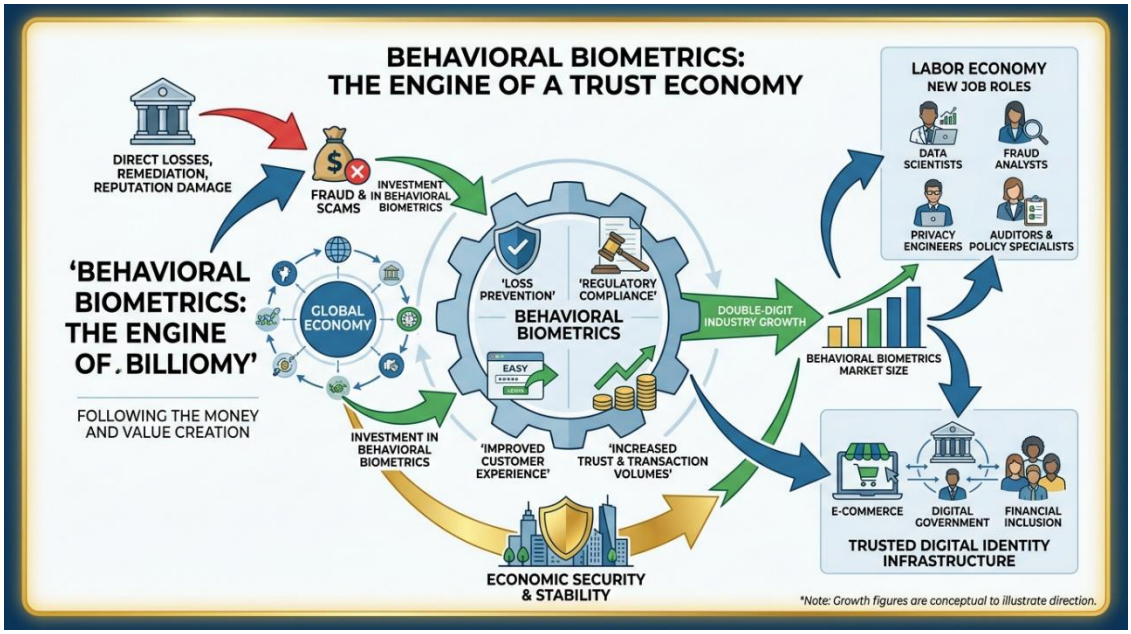

Fig -10: Behavioral Biometrics The Engine of a Trust Economy

It's not just the technology vendors that have an economic story. Good fraud prevention safeguards financial institutions' balance sheets, but also the trust that underpins banking, if people don't feel safe using digital payment, they switch to more expensive payment methods, and eventually all fraud losses are socialized in the form of fees and prices paid by all. Fraud is a parasitic leakage of value from productive activity to fraud networks often international and is a threat to the digital commerce that modern growth strategies rely on. For this reason, governments have increasingly declared large-scale fraud to be an economic security problem. Economies, on the other hand, that create a digital identity infrastructure that is trusted, reduce the transaction costs of all that can be built on top of it, including ecommerce, digital government, and financial inclusion for people historically not served by banks.

There's a labor and skills economy developing around the field, too, with data scientists, fraud analysts, privacy engineers, auditors and policy specialists among the new job categories that didn't even exist 15 years ago. Wherever there's a technology market, there are incentives to tout capabilities, deploy rapidly, and think of data as an asset to be maximized, rather than minimized, and the technology market for the cloud is no exception. The economics of behavioral biometrics' inevitability do not necessarily mean the responsible use of behavioral biometrics is inevitable. History indicates that that outcome is dependent upon governance, which must be demanded, as the following discussion explores.

13. PRIVACY, ETHICS, AND DATA PROTECTION THE QUESTIONS THAT MUST NOT WAIT

Behavioral biometrics, the act of observing people. For whatever purpose it is used, that fact puts it forever in the realm of privacy ethics and society's history with other observational technologies suggests that these issues need to be dealt with at the outset of adoption, rather than after harm has occurred.

Consent and awareness is the first concern. The technology is passive, invisible and users can be enrolled and monitored without their knowledge. Invisibility is a user experience attribute, and a danger for autonomy. For ethical deployment, there needs to be meaningful transparency, which means that there's clear communication that behavioral information is being gathered, what it is, what it's used for and how long it's stored. The trend of data protection law is in the same direction: many key regulations categorize biometric data for identification purposes as sensitive data, and in many of these jurisdictions, explicit consent and in many, affirmative opt in consent. However, the protection of this type of data is not uniform across the globe and in some cases, the definition of this type of data is not clearly defined in legislation explicitly focused on fingerprint and face data.

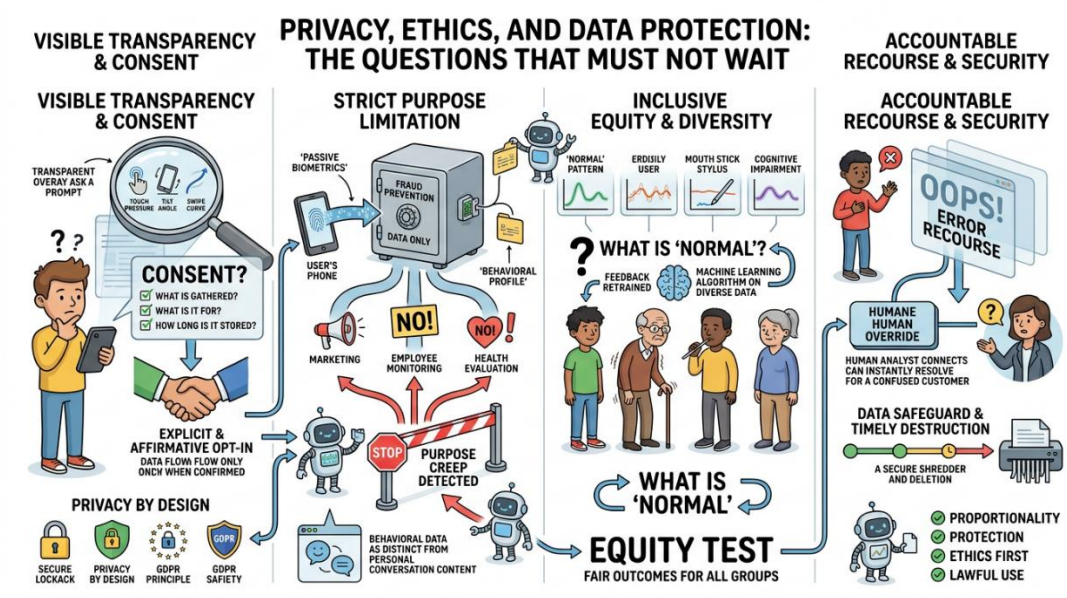

Fig -11: Privacy Ethics and Data Protection

The second worry is that of purpose creep. The behavioural profile which is designed for fraud prevention might theoretically be used for other purposes, such as determining how productive a worker is by their typing patterns, predicting emotional state or health from changes in behaviour or input into marketing systems. Gait and motor patterns can convey information about neurological and physical condition typing dynamics can change due to fatigue, stress or medication. Unchecked use of data collected as a security measure could turn into an unconsented health inference engine. The principle of ethics is purpose limitation: whatever data is collected for security should only be used for security and if it is used for other purposes, it should be brought back to the individual for renewed consent.

The third is the issue of equity among human diversity. Behavioral models are trained to understand what is considered normal for the population(s) they have been trained on. Individuals with motor disabilities or tremor conditions, or individuals who do not interact with systems in conventional ways, may be continually identified as anomalous by systems that were never taught their normal. As older adults, people who use AT and people who share devices within families all have patterns that may be misinterpreted by poorly designed systems as suspicious. If a security technology has a disproportionate impact on a certain class of people, it is not a neutral technology and the disparate impact test must be a continuous test, rather than an afterthought.

The fourth concern is the security of the behavioural data, as well as error and recourse. Profiles should be safeguarded, kept for as long as they need to be and destroyed in a timely fashion. But, since all probabilistic systems make mistakes, there needs to be a quick and humane way to recover for those who are incorrectly marked. There are a series of obligations which have been combined by international biometrics bodies into published principles, including proportionality, consent, protection and purpose limitation, which have been recently updated to include artificial intelligence specifically. The principles are there, as is the unfinished work, which is explored next, in the translation of the principles into enforceable law and practice.

14. LESSONS FROM PAST GOVERNANCE SHORTCOMINGS

14.1 What Leadership Has Historically Gotten Wrong

It is not impossible to speak candidly about the shortcomings of governance in the context of new technologies without pointing fingers at any individual, party or country, as the shortcomings in question are incredibly universal. In fact, the past 20 years reveals a common thread in the way that those entrusted with the care of the public have reacted to game changing digital technologies, and that's the best indicator of what needs to change with behavioral biometrics.

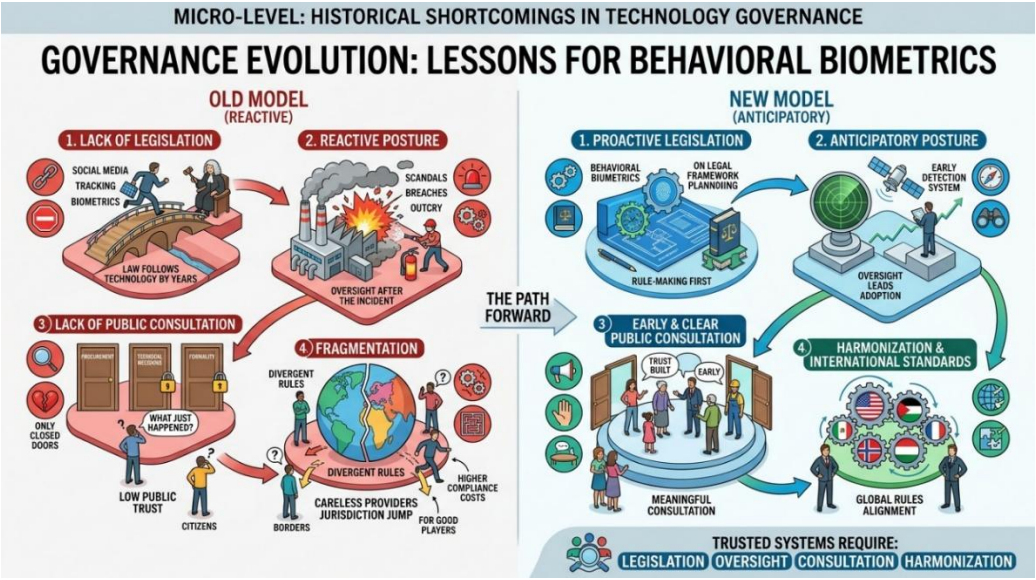

Fig -12: Lessons for Behavioral Biometrics

The first common weakness is the lack of legislation. Social media platforms, smartphone location tracking, facial recognition and large-scale data brokerage were deployed at scale years before any meaningful legal frameworks were put in place to deal with them and over the years, societies have endured harms such as privacy loss, manipulation and discriminatory outcomes that could have been avoided had these technologies been subject to rule-making earlier. The trend continues in the area of biometrics today, the majority of the world's population resides in territories with only indirect protections for behavioural biometric data, via general privacy laws drafted for other purposes, and in some key economies, there is no national biometric privacy law, but rather a mosaic of regional regulations. Technology went first, followed by lawmaking, in years.

Partners Universal Innovative Research Publication (PUIRP)
Volume: 04 Issue: 04 | July - August 2026 | ISSN: 3048-586X | www.puirp.com

The second is a reactive posture; not anticipatory. Typically, regulatory focus has been focused at the end of the deployment when there has been a scandal, breach or public outcry. Fortunately, enforcement of improper collection of biometric data, and poor data protection, has increased in number and severity in recent years, on several continents. The takeaway oversight mechanisms must be able to be in front of adoption trends, not behind them, and must possess mandates, expertise and resources to do so.

The third limitation is a lack of public consultation. Too often, decisions affecting the identity infrastructure, which will impact all citizens, have been made in technical and procurement processes that have been largely opaque to citizens, with consultation limited to formality. Citizens then find out what was done for them, and lose trust, sometimes destroying otherwise good programs. True consultation early and in language that is understood is not a barrier to good deployment, it is essential to public acceptance of deployment that will last.

The fourth weakness is the fragmentation. Divergent rules also impose compliance costs on legitimate providers and service recipients, and provide incentives for careless providers to move to jurisdictions with less stringent rules, where data-driven services can go. A clear gap is the lack of harmonized international standards for the governance of behavior biometric a gap that is only partially addressed by the work of professional bodies in the form of voluntary guidelines.

Notwithstanding all of these observations, it is not as if recent years have not seen real progress in the form of sensitive data classifications, consent requirements and AI governance frameworks in an ever expanding list of jurisdictions, and this does not diminish the challenge of governing fast moving technology. The whole idea of documenting past mistakes is not to point fingers, but to remember today's decision makers on behavioral biometrics have a very clear map of the potholes in the recent past.

15. MEASURING TRUST HOW ACCURACY IS DEFINED, AND WHY REPORTED NUMBERS DESERVE SCRUTINY

Any assertion of the "accuracy" of a behavioral biometric system is meaningless unless there is an understanding of how the accuracy is being measured, and this is the one most valuable analytical tool that a non-specialist can bring with him/her into this field.

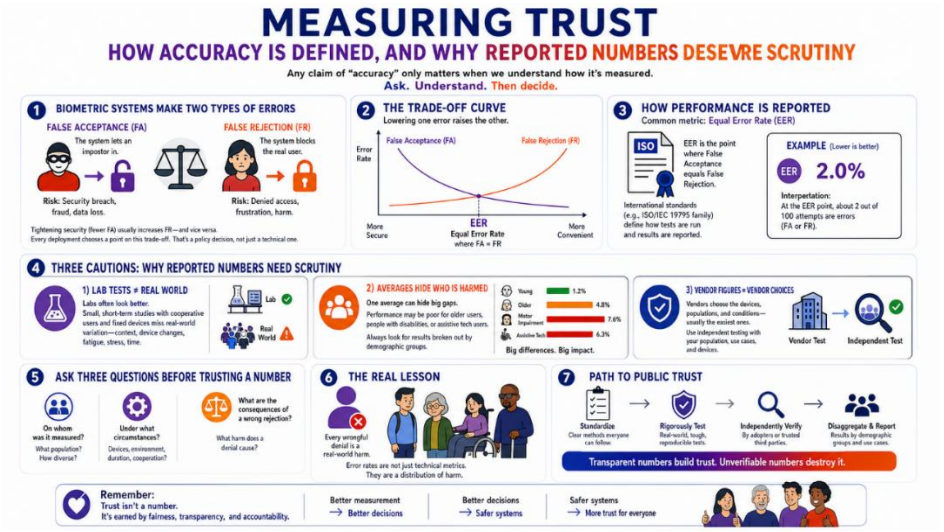

Fig -13: Measuring Trust

Biometric systems commit two types of errors, which are in opposition to each other. A false acceptance is when the system accepts an impostor as the legitimate user and a false rejection is when it fails to accept the legitimate user. A system can be made more secure by making it harder to get in for impersonators, but this means that it will also be harder to get in for legitimate users. Each deployment thus lies somewhere on this trade off curve and the selection is not a technical one, but a policy decision. The performance is often reported by the equal error rate, at which the number of both types of errors is the same, and international standards for performance evaluation, such as the ISO/IEC 19795 family, specify the methodology of such tests and reporting.

Three cautions follow. For one thing, laboratory tests regularly beat the performance of real-world tests. When studies are performed on small, homogeneous volunteer populations, for short periods of time, with cooperative users and fixed devices, the error rates found in the studies are seldom duplicated in the field. Laboratories often don't capture the variation in behavior with context, device, fatigue, and time that is particularly characteristic of behavioral modalities. Second, distributional figures are hidden in the aggregate figures. An impressive average error rate may mask the fact that the system works very poorly for older users, users with motor impairments, and users of assistive technologies and a single headline number tells nothing about who is making the errors. Responsible evaluation reports out performance by demographic groups. Third, vendor-reported figures are made under circumstances which the vendor chooses. The only way to make deployment decisions is on the basis of independent testing by the adopting organisation of their own population, use cases and devices.

The point for the general reader is the attitude of asking three questions when an accuracy statement is made On whom was it measured, under what circumstances, and what are the consequences if someone is rejected in error. The lesson for adopters is that error rates are not just technical metrics, but a distribution of harm, with each time a person is wrongfully denied access to something that is theirs, an error rate. A field that standardizes, rigorously, independently verifies, and disaggregates demographically the evaluation will gain public trust, and one that is based on numbers that can't be verified on the front page of the paper will lose it.

16. MISTAKES FUTURE ADOPTERS MUST AVOID A PRACTICAL CAUTIONARY GUIDE

This discussion is not about governance, but about practice, moving forward from the previous discussion. As organizations and governments begin to use behavioral biometrics in the coming years, they will be tempted to do certain things, and it is easy to predict what those things will be, and the harm that will result from doing them. Now, simply calling these errors what they are, is one of the best things an awareness article can do.

The first is deploy without informed consent and transparency. The technology is passive, making it easier to deploy and ethically eroding. Not only are organizations that enroll users covertly putting themselves at legal risk, as the spread of sensitive data consent requirements across jurisdictions, but they are also building a pool of public outrage that will be released on them when they are discovered. Getting it right is not a big deal communicate to people clearly what is being measured and why.

The second error is to rely on behavioral biometrics as a standalone and or failproof authenticator. The technology is probabilistic in nature and is best suited as one of a number of factors in a defence. Systems that rely solely on behavioral cues to permit or deny access will result in security breaches as well as more obvious lockouts of legitimate users whose behavior has changed due to injury, illness, aging, stress, or

simply some new device. All deployments must have graceful fallback options and quick human intervention.

The third error is to fail to make demographic fairness testing. A system designed for young able-bodied technologically literate users will go out of its way to mistreat the rest of us. Before adopting, and after, the adoption of a language must be tested over age, ability, language and interaction styles and any persistent differences must be treated as a defect and corrected, not as acceptable error.

The fourth is purpose creep, the use of the security collected behavioural data for employee assessments, marketing, health inferences or any other purpose other than what was stated. This is the one and only way to destroy trust and contractual, technical and governance barriers to this path should be erected at the beginning, and not after the scandal.

Fig -14: A Practical Cautionary Guide

The fifth is inadequate data lifecycle governance. Behavioral profiles shall be encrypted, access controlled, kept in accordance with a written and adhered to retention schedule and destroyed upon no longer being needed. Data stored just in case is a liability becoming a liability.

The sixth error is to take vendors' claims on faith. In a fast expanding market, there are bound to be figures of accuracy that are exaggerated and achieved under favourable laboratory conditions. Adopters should require an evaluation on their populations and use cases, and the error rates broken down by user group.

The seventh error is by the policy makers waiting. The takeaway from all the previous technology waves is that governance created at the time of deployment is less costly, less harsh, and more effective than after harm governance.

And an eighth for all of them, for each risk score is a human being on the other end, maybe a scared human being trying to get to his or her own money, and the humanity of the response is part of the system's quality. Technology will last a long time for adopters who don't make these eight mistakes; for others, it will be a re-learning experience to understand why the mistakes were called such.

17. THE GAP WHAT RESEARCH AND PUBLIC UNDERSTANDING HAVE NOT YET RESOLVED

An honest article should not only draw the boundaries of the known, but also of the unknown, and there is a lot of unknown in the field of behavioral biometrics, in both the research and public domain. Their identification can be useful for scholars looking for problems, regulators looking for priorities, and readers looking for the correct modesty with respect to what is known.

The first gap is along the length of the molecule. The vast majority of published assessments of behavioral biometric systems are done over a period of days, weeks or up to months. Human behavior, however, wanders over the years, with aging, sickness, new jobs, new devices. Long-term lifespan studies of systematic stability, adaptive learning and error rates are still limited, and statements about the behavior of these systems over a decade are based more on engineering assumption than on evidence.

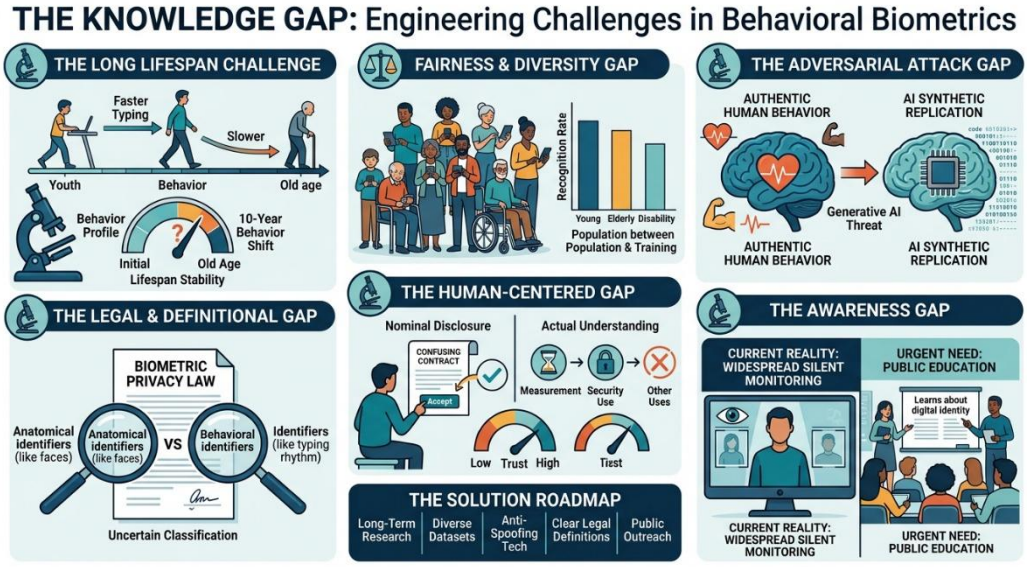

Fig -15: Engineering Challenges in Behavioral Biometrics

The second is related to fairness and diversity. Recent systematic reviews of the literature note that most of the work focuses on the design and performance of the technical systems, with little attention paid to variation in demographic performance, disability user accessibility or cross-cultural validity. Datasets for training and testing systems often fail to adequately represent older people, individuals with motor impairments and people from other than a few countries. Deployments could still pose unquantifiable fairness risk until this evidence base is expanded.

The third gap is the gap of adversarial. With the proliferation of behavioral biometrics, it is inevitable that criminal adaptation will follow, and research into imitating attacks, replaying recorded behavioral data and creating machine-generated synthetic behavior to match the behavior of specific individuals is still in its infancy compared to the potential threat. With the advent of more and more capable generative systems, this question is becoming more and more relevant the long-term competition between behavioural verification and behavioural synthesis is one of the most important open questions of the game.

Definitional and legal gap is the fourth one. Numerous biometric privacy laws were written with anatomical identifiers in mind and it's debatable whether behavioral identifiers, like keystroke rhythms and gait signatures, would be considered anatomical or not. This uncertainty over rights and obligations leaves

individuals and organisations unsure of their rights and obligations and harmonized standards that specifically address behavioural data are largely lacking.

Human centered is the fifth gap. There has been comparatively little research that has investigated perceptions of continuous behavioural monitoring, disclosure formats that lead to actual as opposed to nominal understanding, and the role of trust, privacy concern and perceived benefit in acceptance, although recent studies on adoption have started to make maps of these attitudes. The sixth gap last but not least is the awareness gap the gap between the wide deployment of this technology and the lack of knowledge of its existence among people observed by such technology. That's why there are articles like this one to fill that particular void, but there needs to be public education on the matter, school curricula to teach digital identity, and journalism that can do it accurately. In a society where everyone knows it's a technology that watches everyone that's safest.

18. THE ROAD AHEAD BEHAVIORAL BIOMETRICS AND THE SOCIETIES OF THE FUTURE

For the future, a number of trajectories are clearly set and it is possible to follow them and imagine the world being constructed by every citizen, professional and policymaker.

First is integration in to zero-trust architectures. Modern cyber security is based on the premise that every user, device and session must be treated with suspicion and that trust needs to be continually established and reaffirmed. The continuous identity signal, which the philosophy requires, is provided by the natural sensory system of such architectures, behavioral biometrics. Continuous behavioral verification is poised to become as commonplace as encryption is today as governments and enterprises embark on their migrations to zero-trust designs over the coming years.

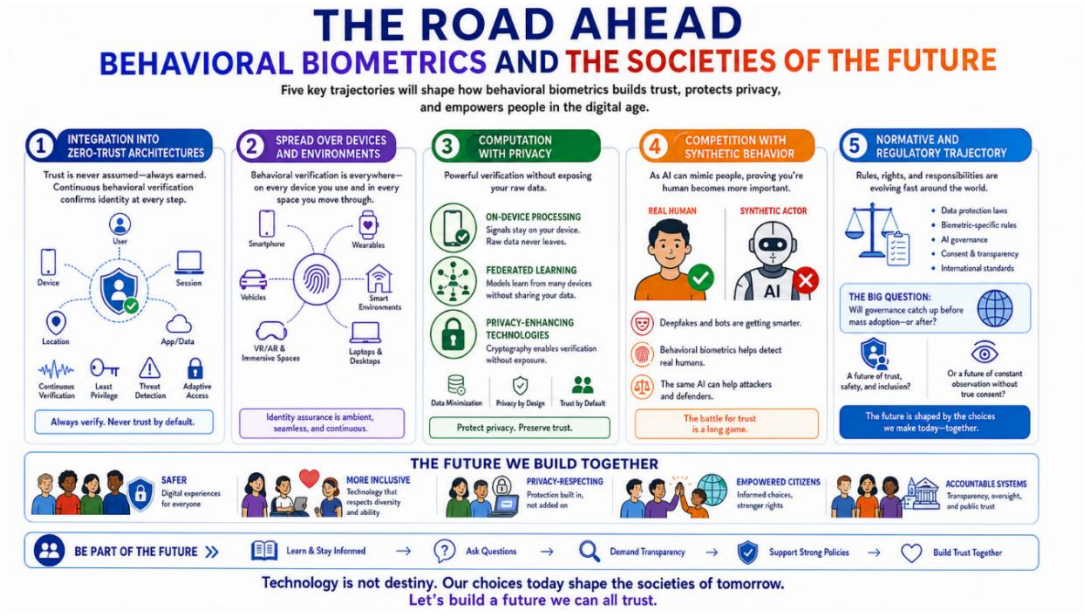

Fig -15: Behavioral Biometrics And The Societies of the Future

The second trajectory is the spread over devices. Behavioral verification is not limited to phones and computers anymore, and is now being explored in wearables, vehicles, smart environments and immersive virtual workspaces, including studies on continuous authentication using a combination of biometric and environmental signals on resource-constrained devices. In such a world, identity assurance is ambient,

spread throughout the objects of everyday life, and the convenience and governance issues outlined above are magnified.

The third is computation with privacy. A body of work that holds promise that could bridge the gap between continuous verification and data minimization is the processing of behavioural signals on the device itself so that no raw data is sent off the device, federated learning approaches whereby data can be used to train models without data being shared, and cryptographic methods which enable verification without exposure. If these methods develop and become a reality, the core conflict of the field protection via observation may be significantly reduced, and the public should demand on-device, privacy preserving designs as the norm.

The fourth trajectory is the competition with synthetic behavior that is deepening. The more generative systems are able to mimic human interaction, the more important it will be to ensure that a real human is involved and behavioral biometrics will play a key role in helping to separate people from ever more convincing software. At the same time, the same generative power will be directed toward combating behavioral verification, allowing for a long technical battle, the result of which will impact trust in the digital world.

The last trajectory is normative. The regulatory tide is clear the number of sensitive-data classifications and consent requirements, as well as AI governance regimes and biometric-specific rules, has proliferated over the last few years across jurisdictions, and international professional guidance has evolved. The open question will be: does governance get consolidated before or after mass deployment. Such a future, where behavioral biometrics will be recalled as a technology that created a safer, more gentle and more inclusive digital life, is very much possible. Is that the future they will look back on it as a time when continuous observation became the norm without consent. It will be the societies that use technology that decide between them by law, demand and awareness and it is that decision that is being made now.

19. CONCLUSION

Behavioral biometrics is a true paradigm shift in the long campaign of human beings to trust at a distance. For decades, digital systems have been used to verify secrets and tokens and keep the people who use them in the dark a stolen password was a stolen identity and the time after logon was a time of institutional blindness. The technology overcomes this blindness by reading the signatures that are embedded in everyday actions, such as the rhythm of typing, geometry of a swipe, cadence of a walk, and so on, and is always available to guard without burdening the person it serves.

This article has followed the technology from its scientific underpinnings of the individuality of learned motor behavior, its main modalities, its technical pipeline of capture, profiling, scoring and adaptive decision making, to its transformative impact on society. For countries, it provides safeguarding of public resources, secure electronic services and opportunities for inclusion of citizens who are not included by traditional security. For enterprises, it eliminates the traditional balance of fraud prevention and customer experience and focuses friction where there is risk, not on all users. For individuals, it offers protection from account takeover and manipulation fraud, reduced security demands in everyday life and specific security for those who are most susceptible to fraud by criminals the elderly and vulnerable. By the time you read this, the losses from frauds will be in the hundreds of billions and the regulatory and commercial pressures will be just as strong, making sure that the adoption process will continue to ramp up.

But the article has balanced the need to not outpace what acceleration must not. A continuous behavioural observing technology has a double edged sword and that good side can only be maintained through governance: informed consent and plain language transparency, testing for fairness across the spectrum of human bodies and abilities, disciplined data lifecycle management, and humane recourse for the inevitably misjudged. The difficulties of previous technology governance, where legislation didn't keep pace with technology deployment, oversight came after the fact, and the public was consulted last, are not only listed here but serve as a warning to those who will follow in the future to ensure that such difficulties will not be repeated. There are still gaps to be filled in terms of longitudinal evidence, studies of demographic fairness, adversarial resilience, legal definition and, most important, public awareness, which is the work of scholars, regulators and educators.

The last word is up to the reader. Behavioral biometrics will impact almost everyone's digital life, and it doesn't require anything to be seen from anyone that's why it's important to understand. What is to be measured, why, and what the standards outlined in these pages are, is what is the best insurance that this amazing technology will be used to secure people, not watch them, quietly, fairly, and by consent.

REFERENCES

[1] Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D. (2021). Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. IEEE Internet of Things Journal, 8(1), 65–84. https://doi.org/10.1109/JIOT.2020.3020076

[2] Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioral biometrics. IEEE Communications Surveys & Tutorials, 18(3), 1998–2026. https://doi.org/10.1109/COMST.2016.2537748

[3] Liang, Y., Samtani, S., Guo, B., & Yu, Z. (2020). Behavioral biometrics for continuous authentication in the Internet-of-Things era: An artificial intelligence perspective. IEEE Internet of Things Journal, 7(9), 9128–9143. https://doi.org/10.1109/JIOT.2020.3004077

[4] Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems, 16(4), 351–359. https://doi.org/10.1016/S0167-739X(99)00059-X

[5] George, D., Dr.T.Baskar, & Dr.M.M.Karthikeyan. (2026). The Grammar of Icons: decoding the origins, meanings, and cognitive power of everyday digital and cultural symbols. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19959167

[6] Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. IEEE Signal Processing Magazine, 33(4), 49–61. https://doi.org/10.1109/MSP.2016.2555335

[7] George, D., Dr.T.Baskar, & Siranchuk, D. (2026). Digital Addiction in Children: economic impact, global age restrictions, and protective solutions. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.18818134

[8] Skalkos, A., Stylios, I., Karyda, M., & Kokolakis, S. (2021). Users' privacy attitudes towards the use of behavioral biometrics continuous authentication (BBCA) technologies: A protection motivation theory approach. Journal of Cybersecurity and Privacy, 1(4), 743–766. https://doi.org/10.3390/jcp1040036

[9] George, D., & Dr.T.Baskar. (2026). India's Unified Payments interface architecture, adoption, and the policy challenges of a public digital payment infrastructure. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.21891881

[10] Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2022). Key factors driving the adoption of behavioral biometrics and continuous authentication technology: An empirical research. Information and Computer Security, 30(4), 562–582. https://doi.org/10.1108/ICS-08-2021-0124

[11] George, D. (2025c). Sanchar Saathi Digital Security versus Civil Liberty in India 's Smartphone Era. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17838468

[12] George, D. (2026a). Digital dividend data taxation's potential to transform India's economy and redefine fiscal policy in the mobile era. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19021896

[13] Yampolskiy, R. V., & Govindaraju, V. (2008). Behavioural biometrics: A survey and classification. International Journal of Biometrics, 1(1), 81–113. https://doi.org/10.1504/IJBM.2008.018665

[14] George, D. (2025b). Digital Watermarking in Cloud Environments for Copyright Protection: A Comprehensive review. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17726895

[15] European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[16] George, D. (2025a). Beyond the dashboard critical perspectives on digital employee monitoring and the paradox of productivity measurement in contemporary organizations. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17702042

[17] Frank, M., Biedert, R., Ma, E., Martinovic, I., & Song, D. (2013). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Transactions on Information Forensics and Security, 8(1), 136–148. https://doi.org/10.1109/TIFS.2012.2225048

[18] George, D. (2026b). Digital Inclusion vs. Fiscal Revenue Assessing India's Per-Gigabyte Data Tax. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.20922074

[19] International Organization for Standardization. (2021). Information technology — Biometric performance testing and reporting — Part 1: Principles and framework (ISO/IEC 19795-1:2021). https://www.iso.org/standard/73515.html

[20] George, D., George, A., Dr.T.Baskar, & Pandey, D. (2026). Digital Dependency and Temporal Distortion: A Critical review of smartphone use, cognitive impact, and Behavioral intervention in Post-Pandemic Society. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19864919

[21] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[22] George, D., & George, A. (2025). How artificial intelligence systems function as digital migrants creating more profound societal disruption than human immigration. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.16112307

[23] Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2021). Behavioral biometrics & continuous user authentication on mobile devices: A survey. Information Fusion, 66, 76–99. https://doi.org/10.1016/j.inffus.2020.08.021