Privacy Analysis of Biometric Data Breaches and Consumer Risk

Adarsh Rai

Carnegie Mellon University: Heinz College School of Information Systems
Privacy in the Digital Age – 94806-A4

4/25/2025

Table of Contents

Introduction

Biometrics have seen widespread adoption in many organizations, which range from fingerprint and facial recognition to veinand iris scans, and they have redefined the current landscape of identity verification and access control among those organizations. Biometrics are held to a higher standard when compared to other security controls due to their perceived security and convenience. However, the increasing reliance on biometrics has introduced new vulnerabilities in the threat landscape. Once biometric traits have been compromised, they cannot be changed and as such pose long-term risks for individuals whose data is exposed. This paper examines the anatomy of biometrics and their implications for consumer identity theft and how organizations can secure their biometric data. It explores the current capabilities of biometrics, current breaches and their implications on consumers, and physical, administrative and technical challenges with implementing safeguards for biometrics, cost-benefit analysis for organizations considering implementing biometrics, and recommendations for organizations and consumers to best secure their data. Using a cost-benefit analysis, this paper offers recommendations for both consumers and organizations. We also propose policies to enhance accountability and resilience in the face of growing biometric threats.

Methodology

This analysis uses a multidisciplinary-based approach to evaluate the security implications biometric authentication systems have on consumers and makes recommendations for both organizations and consumers to better protect themselves. This methodology involves a three-pronged process: literature review through analyzing current capabilities and future trends, breach analysis, and a synthesis of recommendations.

1. **Current Capabilities & Future Trends**
   This first section reviews the current and future trajectory of biometric technologies and draws from various peer-reviewed journals, technical conference papers, white papers, and regulatory documentation. These sources are used to establish the capabilities of biometric systems and to identify trends within the market for new authentication methods.

2. **Breach Analysis and Cost/Benefit Analysis**
   The second section involves analyses of biometric data breaches to understand the implications on consumers and where these biometric systems have failed. The breach analysis was then used to identify technical, administrative, and physical vulnerabilities present across incidents. These findings were then used to create a cost/benefit framework to analyze tangible and indirect consequences of implementing biometric authentication systems.

3. **Recommendation Development**
   In the third section, insights are synthesized from the prior two sections. These recommendations include recommendations for consumers and organizations alike. Finally, policy recommendations are developed as a framework to address regulatory, administrative, managerial, technical, and physical vulnerabilities to provide comprehensive guidelines for securing biometric systems should they be implemented.

Current Capabilities and Future Trends

Biometric authentication is becoming increasingly integrated into our modern digital ecosystems. Understanding its current capabilities as well as the projected changes that this technology will see in the coming future is essential for understanding risks and creating effective solutions to mitigate these risks. The rapid development and evolution of new technologies creates new challenges and risks for organizations and consumers, respectively.

Current Capabilities

Current capabilities of biometric technology encompass a vast number of potential authentication mechanisms from iris, retina, gait, palmar geometry, tongue scans, voice recognition, facial recognition, speaker, and keystroke patterns. These tools extract either physiological measurements or behavioral traits that are compared against established templates in the authentication process. Advancements in technology given the power that artificial intelligence (AI) and machine learning (ML) pose leaves some of these mechanisms less desirable or effective than others. Analyzing the capabilities and limitations of biometric authentication aids in determining effective organizational policy for authentication, but also poses concerns for consumers if there is a data breach because biometrics cannot easily (if ever) be changed. Usage of biometrics for authentication has grown rapidly across various sectors. Financial institutions, healthcare providers, border control agencies, and technology companies have increasing reliance on biometric systems for enforcing access control. This, coupled with the ongoing expansion of the Internet of Things (IoT), attack vectors have grown in an order of magnitude for capturing the real-time transport of this biometric data. Recently, electroencephalography (EEG) has been growing in prominence as a biometric tool as a result of both 5G, IoT, and edge computing, which detects the electrical activity of the brain (Beyrouthy et al., 2024). Innovations such as these propose low probabilities for type II errors, where users would be authenticated when they should not have been, but poses unique challenges for encrypting data, but also ensuring hardware and firmware are securely coded and built and pushes the envelope for what is acceptable as an authentication mechanism in terms of biometrics.

Given the advancements that have occurred within the past few years in generative AI with capabilities to create convincing deep fakes, biometrics such as voice recognition and facial recognition are likely to become less reliable and may fade out in favor of more advanced biometrics, such as iris and retina scans, palm vein scans, or EEG as mentioned above. However,

to capture these biometrics, organizations will have to invest in specialized equipment to capture these measurements. Although they have a high degree of accuracy and are difficult to replicate, they may be onerous and burdensome to invest in, especially for organizations with small profit margins. However, cancelable biometrics, which allows biometric templates to be mathematically altered and can be revoked if compromised, are becoming more prominent as a method to safeguard biometric data in tandem with genetic encryption algorithms or multimodal authentication when applicable, which analyzes multiple biometrics for authentication (Fatima et al., 2024).

Future Trends

Acknowledging the trends in the market, the future of biometrics suggests a shift to multifactor biometric systems to adequately protect users and may combine both behavioral and physiological templates. Additionally, there are suggestions for decentralized identity management via the blockchain, but current models lack integration of zero knowledge proofs, which would functionally validate a biometric measurement without revealing it to the other party (Thorve et al., 2023). A structured system that relies on these zero knowledge proofs would also require that system infrastructure stay relatively stagnant to integrate, but could provide a reliable framework to address centralized biometric authentication in the future. However, zero knowledge proof capabilities have not yet materialized and will be key to implement for protecting data in a post-quantum computing world where 61 percent of businesses consider themselves not prepared to migrate to post-quantum cryptography standards (DigiCert, 2023). Similarly, maintaining biometric data storage decentralized and "device only" may become a dated practice. Some additional capabilities we may see in the future include embedding confidential data into quantum image representations, which may alter how biometric templates are created (Min-Allah et al., 2022).

Based on the trends in market and innovation within the biometric industry, biometrics that may be considered more invasive but are more difficult to replicate and are likely to become the standard as our society moves to be passwordless due to post-quantum technology, which will redefine security standards and implementations as we know them. Revocable and resilient methods will be necessitated to safeguard biometric data as it becomes increasingly used. Risks and responsibilities for utilizing biometric authentication for consumers are broad and place a hefty responsibility on organizations to adequately protect their data, but are also potentially more invasive as the need for accuracy increases, such as with EEG or retina scans.

Breach Analysis Implications for Consumers

Biometric breaches are becoming a growing concern in the current digital landscape. More organizations are adopting fingerprint scanning and face scanning and with it, the threat landscape expands in proportion at a greater magnitude. Breaches of personally identifiable information (PII) and biometric data expose people to life-long identity theft and even recurring privacy breaches. There is a need to focus on securing these systems that handle and process this

sensitive biometric data.

Breaches of biometric data have been occurring for many years. One major example includes the US federal government Office of Personnel Management. In the summer of 2015, the office released a statement that over 21.5 million federal workers had their information breached, which included their social security numbers and other PII (Greenberg, 2015). Of those 21.5 million, the Office of Personnel Management estimated that anywhere from 1.1 million to 5.6 million fingerprints were exfiltrated. Not only is this breach of biometrics devastating for the employees that were affected, but it also poses a national security risk: many of these fingerprints belonged to members of the government that held security clearances. The threat actor dubbed "X1" (Fruhlinger, 2020) could easily use these fingerprints to commit identity theft by bypassing multi-factor authentication (MFA) that uses these biometric signatures and threaten the national security of the United States.

Similar systems globally are also at risk of these breaches. The biggest biometric identification system, called Aadhaar, is utilized by India to store basic information of residents of India and assigns each of these residents a random 12-digit number and registration card. The information that is stored in Aadhaar includes biometrics data such as iris scans and photos, as well as fingerprint scans (Ayyar, 2018). In October of 2023, Resecurity, a cybersecurity organization that specializes in endpoint protection, risk management, and threat intelligence noticed around 815 million "Indian Citizen Aadhaar and Passport records" (ETtech, 2023). Cybersecurity researchers were able to find a leaked sample of the data set, which included PII of Indian residents. Although not specifically mentioned, one could imagine that biometric data would have also been found within that sample given the Aadhar system includes data of all residents of India–some 1.4 billion people (Government of India, 2023).. A biometric breach on this scale is cause for alarm for the whole country of India, as identity fraud can run rampant with even a small sample of the dataset being released into the public. Systems similar to these are also being adopted in all industries. The compounded annual growth rate of biometric authentication technology is 12.3 percent and expected to grow to be worth 84.9 billion by 2029 (Markets and Markets, 2023). As the usage of these systems grows, so do the risks of breaches and turmoil that could ensue for consumers in their personal lives should it be obtained and used maliciously.

A Future Look at Biometric Breaches

In the future, we face many life-altering outcomes based on how biometric breaches may change or proliferate. As technology advances and we develop new biometric measurements, committing identity theft could be an easier task than it once was. We are already seeing instances of AI being used to commit identity theft through the use of deepfakes. In the year of 2024, there was a 1,400 percent increase in deepfake attacks across the world (Borak, 2025). Perhaps not all biometrics may be susceptible to deepfake attacks, but not every organization will utilize the most robust or secure biometric authentication mechanisms.

For organizations that use less robust biometric authentication, AI will become more

advanced and proliferate in its use by the public, which creates opportunities for threat actors to take advantage of its accessibility and conduct widespread identity theft. A critical example of a deepfake being used to commit identity theft is the recent North Korean who was caught working for KnowBe4, a cybersecurity solutions organization. The organization listed job postings for a software developer the individual applied using a stolen identity card with an AI-enhanced photo to look more like the North Korean who was interviewing for the position. He passed several interviews, accepted the job offer, and ultimately installed malware on their servers (Sjouwerman, 2024). Fortunately, he was caught before any damage was done internally to the organizations. Although better vetting could have prevented this from ever happening, the fact that it is occurring at present is an ill omen. The future of attacks utilizing deepfakes to trick systems will only grow, especially with the growing number of applications coming out that allow users to use a real-time face swap using AI (James, 2025). However, this is still an emerging technology that can be mostly beaten as of now because only threat actors with a high amount of resources can afford to use the more advanced software that allows face-swapping to appear seamless. Unfortunately, the implications of this growing technology are immense: if they are good enough to deceive real people, then it is safe to assume that biometric systems may also be fooled by this unless very specialized equipment and cameras are used in the authentication process. As time passes, we will see an increase in use of these deepfake technologies to breach these systems and have the potential to cause widespread havoc unless more secure, deepfake-proof biometric authentication methods are used.

Biometrics are typically stored in mathematical representations of the features of characteristics of a biometric scan which are referred to as templates. This can include facial images, voice recordings, or fingerprint scans (Choi, 2022). These templates are encrypted to prevent access from threat actors if the database they are stored in is breached. In the near future, more advanced attacks will involve quantum computing given Microsoft's recent announcement of their Majorana chip (Bolgar, 2025). Unfortunately, quantum computers will present a way for well-funded threat actors to bypass encryption techniques as we know them unless organizations move to more secure cryptographic systems due to their efficient and advanced computations, which will then force previously safe encryption algorithms into obsolescence (NIST, 2025). Quantum computing also offers a popular vector attack referred to as the "store now, decrypt later," attack which enables threat actors with breached biometric data to decrypt them when they achieve enough computational power. (McGowran, 2022). Without post-quantum cryptography techniques, threat actors could successfully decrypt these templates and utilize them to bypass the biometric portion of the authentication sequence.

New advancements in quantum computing presents a growing need for organizations to adapt to quantum-resistant algorithms. If one of these attacks are successful and the biometric data is breached, then all individuals who are affected will be able to seek no remediation–one cannot reset their biometrics as easily as a password. This is a future that organizations need to prepare for. Unfortunately, few organizations are prepared to enact plans for post-quantum cryptography within their data storage protection procedures (DigiCert, 2023).

Pain Points in Biometrics and Where Failures Occur

There are many pain points when it comes to successfully implementing and protecting biometric data. The difficulty of it is exasperated by the current evolving threat landscape and the growing complexity of receiving and transmitting biometric data. Furthermore, these challenges can become even more difficult when inconsistent policy enforcement, inadequate technical safeguards, and limited employee training can create a significant gap in a systems security.

One of the major difficulties within policy includes insufficient transparency and accountability within these organizations. This prompted the Federal Trade Commision to release a statement warning organizations about the misuse of biometric information and its harm to consumers (FTC, 2023). Recently, the FTC has brought enforcement to photo app makers like Facebook, stating that they are misrepresenting how they use their facial recognition technology (FTC, 2023). Until organizations act transparently and take accountability for how they mishandle biometric data, consumers will bear all of the burden in the event of a data breach and are likely unable to seek much, if any, repercussion.

Unfortunately, safely storing biometric data may be the most difficult , yet important task an organization undertakes, especially when operating within fiscal, hardware, skill, or implementation limitations. In addition, these systems are vulnerable to many errors, such as failure to enroll, false acceptances and rejections, and spoofing (OVIC, n.d.). Additionally, there are seven different opportunities for attacks on all biometric authentication systems. A few notable ones include: physical damage to the scanner itself, replay attacks could be used to resubmit the data extracted, features can be overridden with different values to gain access, trojan horses used to replace the matching mechanism and assign high scores for all scores, decision overrides, database communication interception, and tampering with either the features submitted or the template itself (Singh & Kant, 2017). Until there are adequate protections to prevent these attacks from occurring, there will always be a technical risk associated with storing and using biometric data for authentication. Although there are opportunities where blockchain technologies that utilize zero-knowledge proofs–which do not directly exchange biometric data–could be implemented, this has not yet been realized in a scalable way for organizations to utilize (Thorve et al., 2023).

From an administrative perspective, many organizations are also not properly trained for interacting with biometric systems. The FTC warns that any organization that fails to comply with the FTC on ensuring employees who interact with these systems are properly trained, then they may be in violation of the FTC act. Adhering to this act includes assessing foreseeable harms and adequately implementing tools to reduce or eliminate those risks, evaluate practices of third-party vendors, provide training for those interacting with biometric data, and monitoring the technologies used in conjunction with the biometric systems (FTC, 2023). Unfortunately, financial constraints and technical debt may hold an organization back from implementing secure biometric systems. Depending on the amount of data an organization plans to use and keep with these biometric systems, costs can rise exponentially given hardware, software, and labor costs.

Outside of technical and administrative concerns, physical breaches of biometric systems is also an issue for organizations who store their biometric data on their premises. Organizations must be able to invest in security technology such as security cameras or robust locks, having proper access controls within that area where the data is being collected, and also vetting employees to ensure that there is possibility for them to break into these secure areas and maliciously tamper with the data (FDC, 2025).

Enforcing proper access controls both physically and technically to access this data can be prohibitively expensive for smaller organizations. Fingerprint scanners cost anywhere from $45 to $500 (Clark, 2017), more secure iris scanners may cost several thousand dollars (CardLogix, n.d.), and installing an access control vestibules can be vastly more expensive, with some vestibules starting from anywhere from $10,000 and $30,000 and could be even higher depending on the features implemented (Total Security Solutions, 2021). Implementing these technologies at scale can be a major expense for organizations considering the cost of the hardware, software subscriptions, and the personnel needed to maintain and audit these devices. Even organizations that are well-funded will try to cut costs where their risk appetite is not exceeded. Idealized implementations of these systems are likely few and far between.

Security Implications and Cost/Benefit Analysis

As with any novel technology, the business case demands justification for taking a specific action. In a world of scarce resources, biometric technologies must sustain scrutiny in reaching a consensus on their implementation. Biometrics offer a number of benefits as well as pitfalls, especially with respect to consumer privacy. One compelling case in defense of biometrics is to crack down on fraudulent representations of individual activity, wherein organizations must "…begin to estimate the benefits and costs of implementing a biometric analytics capability that looks to address the problem of fraudulent records in a biometric data store" (McKenna & Sarage, 2015).

Historically, biometrics followed the traditional logistic "s-curve" of technological adoption since its introduction; starting with slow and gradual adoption, eventually leading into an explosive exponential growth, then leveling off as the technology saturated the market. Currently, a consumer would seldom encounter a device that does not integrate at least partial biometrics into its technology stack. For example, the smartphone: it initially was lacking in features compared to today. Its original iterations were not all too concerned with biometric features. Future renditions of smartphones began to install biometric collections via mediums such as optical fingerprinting, facial recognition, etc. Nevertheless, prior to manufacturer interest in biometrics, there had to be some form of assessment of the technology in the problem domain: the "… slow rate of adoption suggests that some critical factors need to be addressed to help the user decide to either use or not use a new biometric technology after doing a cost/benefit analysis" (Ngugi, 2011, pp. 20). The costs of biometrics are indeed very real, both in terms of dollars and intangible implications, and must be considered for any interested organization prior to implementation. Unfortunately, due to the nature of biometric data and technology, the burden of securing this data falls solely on the organization and not the consumer, even though consumers bear all of the risks associated with biometric data breaches.

Costs of Biometrics

To collect the costs associated with biometrics, it helps to examine an organization from a holistic viewpoint. Biometrics are often marketed as means to enhance security, so they should be scrutinized from this lens. Three active categories for assessing the costs of biometrics are direct implementation, risk management, and compliance which will be discussed below.

Implementation Costs: Procurement, Installation, and Calibration

Beyond the obvious price tag of acquiring devices and installing them, biometrics must be maintained as any typical ongoing information and operational technology. The retail cost of individual devices and specific implementations vary by complexity and manufacturer offerings.

There are also distinctions that can be made on each biometric system based on capability. Biometrics inputting more data types must necessarily collect, parse, and process the inputs of multiple modes. Thus, the tuning costs for multi-modal systems impose additional constraints at the same time they claim to deliver more security: "However, combining different biometric traits induces some drawbacks as the increase in complexity of the global system leads to a higher cost, longer verification time and also lower user convenience" (Allano, 2010, pp. 884).

Risk Management Costs Risk Management

Personnel in various organizations possess differing degrees of clearances and authorizations once they are authenticated to access a given resource. Among considerations of confidentiality, budget, and risk reduction, organizations must make a conscious effort to upgrade existing infrastructure to implement biometric capabilities within the context of their risk posture. Resource planning to accommodate biometrics at the strategic, operational, and tactical levels would become a perpetual task for the adopting organization, which consumes valuable time from management.

Regulatory Compliance

While biometrics is a recent emergent technology that was not foreseen by the founding members of the US, it is nonetheless under regulation across multiple jurisdictions. Due to its recency, biometrics and modern notions of privacy are both held up against the interpretation of case law: "The word privacy, like the word biometrics, is nowhere to be found in the text of the U.S. Constitution. An obvious point needs stating: Just because something is not in the text of the Constitution does not mean that it is outside the Constitution's authority or protection" (Woodward, 2008, pp. 359). Based on the litigants, specifics of the case, and consumer sentiments at any point in time, biometrics exist shrouded in a veil of uncertainty regarding their legality. Therefore, litigation and legal costs related to the "legally fuzzy" status of privacy apply.

Additionally, the US notoriously lacks a blanket regulation or framework to govern consumer privacy. "While in the United States, no general and comprehensive federal law regulates the handling of all privacy-sensitive information, such as biometric data, some states have introduced their own laws. Representative for these, we emphasize the California Consumer Privacy Act (CCPA)" (Meden, 2021, pp. 4173). Despite the absence of explicit federal guidance on the question of biometrics, there are still government-wide standards enforced by agencies handling sensitive information. A prominent example is the array of Federal Information Processing Standards (FIPS) publications maintained by the National Institute for Science and Technology (NIST). On the consumer end of compliance, the closest known regulation to offer

protections is the CCPA, which strictly defines data handling practices for organizations that engage in commerce with Californians, including biometrics under its authority. A similar compliance standard is the Biometric Information Privacy Act (BIPA) enacted in Illinois, which requires informing the individual of the data used, the length it is kept, and obtaining their written consent (ACLU Illinois, 2021). A practicing business must weigh the costs of compliance when considering biometrics.

Benefits of Biometrics

Organizations will continue to search for more secure and user-friendly methods of authentication while minimizing friction with the user. As a result, biometric authentication has seen rapid growth. The benefits of implementing these frameworks include improved accuracy, greater convenience, reduction in fraud, and resistance to spoofing. The subsequent sections examine these benefits in detail.

Improved Authentication

Biometrics can be used to secure existing authentication schemes by introducing a unique, difficult-to-spoof factor into the equation: "The use of biometrics in two-factor and multi-factor authentication systems is an extremely important consideration for banks and payment providers" (The Business Case for Biometric Authentication, 2018). In many cases, reduced intrusion events are correlated with the implementation of 2FA and MFA schemes. If account access incidents are reduced after the implementation of biometrics, this may enhance privacy because sensitive account information becomes more out of reach for unauthorized individuals.

Even with the existence of deprecated biometric systems, innovative solutions promise to improve the status quo with mathematically-provable secure protocols, including those with perfect forward secrecy: A "… novel two-factor biometric authentication protocol enabling efficient and secure combination of physically unclonable functions … enables the participants in the protocol to achieve PFS [Perfect Forward Secrecy]" (Irshad, 2021). Using research to advance developments in the biometrics field helps keep confidence in the systems deployed by organizations, and continues to provide an optimistic outlook for the security of the technology overall.

Convenience

To the end of authentication, users can present features they know, have, or are. "To quickly perform verification of a subject or to perform identification against a watch list, government agencies and other users of these systems maintain large databases of digital biometric records" (McKenna & Sarage, 2015). Biometrics are viewed as convenient to many organizations during the validation phase of authentication, including government entities. Some users may find convenience and comfort in using their physical traits as readily accessible means to authenticate.

Fraud Reduced

Over the course of regular business, firms can find applications of biometrics in securing their systems. “Over 50% of the study participants experienced reduced fraud as a result of deploying biometric authentication and 80% also achieved increased compliance” (The Business Case for Biometric Authentication, 2018). Based on a survey asking those in a management capacity, respondents self identified the (positive) results of enabling biometrics. The impact on fraudulent instances in their business is stated to be non-negligible.

Difficult-to-Spoof

Biometric features are not easily shared between individuals. Large groups of people possess commonalities, but unique ones, which are difficult to copy and abuse without invasive procedures. “Connolly maintains that while it may be difficult for an employee to remember dozens of passwords, it is very unlikely that they will forget or misplace their thumbs needed for logging in” (Dike-Anyiam & Rehmani, 2006, pp. 34). Unlike other factors of authentication, biometrics utilize a trait of a user that cannot be duplicated without great effort. This comes in addition to the convenience of not forgetting the factor itself, since it is tied to the physical person

Risks of Biometrics

Object Permanence/Immutability

Once stolen, biometric features become difficult, if not impossible, to amend due to the nature of biometrics being immutable–they cannot be changed like a password can. Authentication methods based on biology must be non-invasive to not cause physical harm to the end user. Altering such features potentially involves damaging the subject. If stolen, revocation of personal biometric traits is unlikely.

Storage Vulnerabilities

Consolidating user authentication data as sensitive as biometrics can pose a very large risk to the storage processor. The nature of biometrics, building off immutability, makes stolen biometric credentials valuable targets since they can be used in future campaigns. Centralized repositories of biometric data are lucrative targets for attackers and have very high impact if breached.

False Positives & False Negatives

There are security gaps in the form of false positives (approved), and frustration with legitimate users experiencing false negatives (denied). The authenticating biometric system assumes an implicit denial of all transactions. Two parameters, false acceptance rate (FAR) & false rejection rate (FRR), must balance a delicate line between sensitivity versus error rate in the biometric system. False positives potentially elevate attackers into an authorized status, thus compromising the organization. False negatives flag legitimate users, which incurs additional processing costs and loss on personnel time. Selecting the appropriate level of FAR and FRR is a matter of risk appetite weighed against organizational goals: “For example a military organization which is

highly security conscious may sacrifice FRR for FAR while a university system may sacrifice FAR for FRR" (Ngugi, 2021, pp. 26).

Functionality Repurposed

Biometrics may be repurposed to provide avenues for surveillance, profiling, and/or tracking and can be conducted on already obtained biometric–outside the scope of the original or intended use. Because biometrics are sensitive and highly personal, they are perceived as valuable to authorities in enforcing their agenda. "But from a perspective of political styles and forms, the turn to biometrics is very significant. It is significant, for one thing, because of the new forms of surveillance it opens up—a theme that has been explored at great length" (Walters & Vanderlip, 2015, pp. 14). After having already been collected, biometrics can serve other purposes, beyond the ones stated at the point of collection. Biometrics integration in a society may also point to telltale signs of surveillance, profiling, and tracking using unique and personal information, which can be abused to suit the needs of any regime.

Algorithmic Bias

different demographic groups experience varying levels of performance using biometrics, largely due to available training data. Potential for discriminatory access barriers.

Biases within sourced training data can be bred into the algorithms used to validate true biometric authentications. In a way, biometrics integrated with flawed accessibility is a vehicle to exacerbate existing social inequalities. "However, since different types of biases may be involved in empirical evaluations, researchers are increasingly looking into privacy enhancing techniques that offer formal (quantifiable) privacy guarantee" (Meden, 2021, pp. 4153). Nevertheless, researchers are seeking answers to offer more privacy-focused solutions in biometrics, including when collecting samples and data points to increase representation.

Tangible vs Indirect Implications

When assessing the value or impact a biometric system may have on an organization and its consumers the tangible and indirect effects must be enumerated. Organizations should consider all of these tangible and indirect costs before implementing biometric solutions into their authentication and authorization suites and whether they can reasonably afford the implications these technologies have in fiscal terms. Additionally, they should consider if they can reasonably protect their consumers from biometric breach in addition to measuring these indirect and tangible implications on the organization.

Indirect Implications: Risk Management & Compliance

Indirect implications manifest themselves in the areas of risk management and compliance. Risk Management is a holistic improvement of system architecture when incorporating biometrics does not necessarily translate into real dollar terms. It functions as a tool to enable and support organizational strategy, but can become increasingly complex and burdensome as technological systems grow in size and difficulty to secure. Additional resources will likely be

required to adequately review and create controls for increasingly complex biometric authentication systems as they evolve.

Similarly, Compliance is an organization's adherence to laws and regulations. Compliance risks are difficult to quantify. Litigation expenses are not easy to estimate when regulators sue, and further uncertainty exists if cases proceed to trial. It is unknown what legal implications biometrics may have on consumers and what laws may be enacted in the future in the event of data breaches and will be difficult to prepare for.

Tangible Implications: Implementation, Infrastructure, Maintenance, Training, and Liability

Tangible implications are easier to quantify monetarily and be attributed to operational costs. These include implementation, needed infrastructure, ongoing maintenance and personnel needed, user training, and insurance or indemnification expenses.

Implementation represents up-front costs for adding biometric authentication capabilities into an organization's existing authentication infrastructure. Given the cost of biometric readers, this can quickly become a very costly investment. It could be considered a cost-saving mechanism in cases where fraud prevention is most important for an organization or government entity's risk management strategy and could outweigh the cost of implementation (McKenna & Sarage, 2015).

Infrastructure upgrades are usually needed to support implementation of biometric authentication systems. Without standardized infrastructure, systems may face compatibility and thus present issues with vulnerabilities or performance bottlenecks. For example, typing pattern biometrics would necessitate standardization to gain widespread support from mainstream manufacturers to be viable in an organizational setting (Ngugi, 2011, pp. 27).

Ongoing maintenance is arguably the most critical component of tangible costs after implementation and standardization in architecture. Organizations must plan for personnel needed to implement software updates, hardware upgrade, and calibration of sensors. Over time, this can grow to be increasingly expensive. If using a decentralized system, similar investments must be made in securing the decentralized system. If an organization wishes to implement high-quality analytics capabilities, they will face development, production, and sustainment costs to similar effect (McKenna & Sarage, 2015).

User training will require an onboarding procedure to validate existing users across an organization. While a temporary cost, the registration process is necessary for all future usage of biometric devices. Organizations will need to ensure that both administrators and end-users can interact with the systems intuitively and safely. This component is key to adoption and maintenance of the authentication system.

Lastly, liability or insurance and indemnification are financial risks present to an organization and are closely tied to risk management strategies. Because biometric authentication introduces new privacy concerns and risks for consumers, organizations may face increased liability coverage limits. Additionally, their corresponding premium rates will also increase depending on the underwriter.

Recommendations to Ensure Biometric Security

Authentication with biometric systems offers unparalleled convenience for users. Although uses such as facial recognition for unlocking a phone or fingerprint verification for accessing financial data are designated as "seamless" interactions, they come at a cost of permanence. In the event of a breach, biometric identifiers such as irises, fingerprints, and facial structures cannot be revoked once compromised. This enables adversaries to exploit compromised templates for life. Biometric data & processes are also opaque, with users often having little to no visibility into how their data is stored, shared, used, or protected.

As demonstrated by our prior analysis, attack surfaces have been dramatically exacerbated with the integration of biometrics into critical infrastructure. Misuse of generative AI technologies has resulted in deepfake and voice cloning epidemics, as witnessed by a notable incident of a finance worker being coerced into paying $25 million to cybercriminals that impersonated an entire executive board of a multinational firm (Chen and Magramo, 2024).

Necessary steps for improving the current state of biometrics demand more than patchworks of technical fixes. Instead, a systematic, multi-layered implementation is necessary: one that spans the entire lifecycle of biometric data and caters to the needs of involved stakeholders. To address this quasi-dimensional threat landscape, our recommended strategies are categorized across three interdependent levels: consumers, organizations, & regulatory bodies.

Recommendations for Consumers

Consumers play roles as both contributors and victims of biometric systems. While they contribute a significant portion to the data lifecycle, individuals often lack the tools, information, and leverage to meaningfully protect themselves. These recommendations are designed to help consumers reduce their exposure and take back some degree of control, minimizing possible attack surfaces.

Not all biometric systems are created equal. Many commercial applications collect biometric data without clear justifications, retention limits, or on-device processing. Whenever possible, consumers should opt out of biometric authentication for apps and services that rely on cloud-based storage or fail to clearly define their data handling policies. Users should instead consider engaging with systems that possess device-only biometric processing. Popular examples include Secure Enclave from Apple and Android's Keystore system. These systems store biometric templates in isolated hardware modules (Trusted Execution Environments, TEE) and never transmit them to external servers (Fatima et al., 2024). Localization of biometric data in this manner reduces the attack surface.

Certain policies and measures do exist to protect consumers, such as The Federal Trade Commission issuing warnings for misleading biometric data practices (FTC, 2023). However, personal awareness provides higher leverage and, in turn, control over biometric security. Consumers should review privacy policies from services that ask to opt for biometric features. In

particular, consumers should focus on how long biometric data is stored, who the data is shared with and for what purpose, and what options are available for deletion. If a service cannot explain its biometric usage in clear language, users should abstain from enrollment. They can utilize helpful resources such as browser extensions - *Term of Service*; *Didn't Read*, or the Mozilla Foundation's *Privacy Not Included* campaign to interpret complex legalities and discern their individual rights.

Although current technology does not cater to industry-wide biometric revocation, developing models that offer "cancelable biometrics" are a potential solution. These systems will allow biometric templates to be mathematically adjusted, and introduce the ability to be changed if compromised–a technique akin to a password reset, but with greater complexity (JHU, 2018; Fatima et al., 2024). A caveat to the current research is that "in crypto-biometric keys, the entropy contained in the biometric reference limits the entropy of the key as compared to traditional cryptography keys" Amine Hmani, Petrovska-Delacretaz and Dorizzi (2024). This means that the security of cryptographic keys created from biometrics is limited by how unique the biometric data of the individual is, which can potentially leave them weaker than traditional cryptographic keys.

In addition to technical solutions, social and legal pressure may also impact how biometric data is handled. Public pressure from lawsuits have urged major tech companies such as Meta to reduce their facial recognition usage in recent years (FTC, 2023). Organizations like the *Electronic Frontier Foundation* and *Access Now* often release petitions for users to attest and show support for Privacy centric regulations. Participating in public advocacy is an effective way for users to create large momentum and increase the social pressure around implementing sufficient guardrails to better protect user data. Below is a matrix created to illustrate the false positive rates, potential risks from exposure, and abuse cases if the biometric data is leaked.

Figure 1: Biometric Systems Matrix

Biometric System	False Positive Rate	Risk from Exposure	Potential Abuse Case if Leaked
Fingerprint Recognition	15.9% to 28.1% (Koehler & Liu, 2020)	Moderate - Exposed templates can lead to identity theft	Identity theft, fraud, bypassing security systems
Facial Recognition	Best algorithms < 0.2%, Market Algorithms 48% - 62% (Raposo, 2023)	High - Can be captured from a distance, often without consent	Surveillance for unauthorized tracking, privacy invasion
Iris Recognition	<0.1% (Burt, 2023)	Low - Requires direct interaction but can be intrusive	Unauthorized surveillance, stalking, potential identity theft
Voice/Speaker Recognition	Up to 7.4%, varies with background noise (Zhou, 2018)	Moderate - Easily spoofed with pre-recorded voices	Impersonation, unauthorized access, fraud
Gait Analysis	Greater than 5% under ideal conditions (Birch, 2020)	Low - Requires movement and specific sensors	Tracking and surveillance, even in public spaces
Multimodal Biometrics	<0.5% (improves when combining facial and fingerprint recognition) (Haider, et al. 2023)	Moderate - More accurate but requires storage of multiple datasets	Identity theft, combined attacks from stolen datasets
Vascular Pattern Recognition	1% to 15% (varies by age & activity level) (Sinha, 2024)	Low - Difficult to replicate, but sensors can be targeted physically	Bypassing security checkpoints, surveillance of high-security locations

Recommendations for Organizations

Consumers are the origin of biometric data and, as a result, organizations become the custodians of biometric systems. Investing the necessary resources for protection of data at rest and in transit is their responsibility entrusted to them by their consumers and shareholders. These recommendations range from actionable suggestions to long term shifts in preparation for technology overhauls.

The primary risk of biometrics is the irrevocability of compromised biometric templates. Biometric salting is an approach that adds randomness to the biometric template, which obscures original data and prevents exploitation. To aid in this, organizations also have the ability to set internal guidelines for biometric data handling. Minimization of biometrics is key: companies must only make an effort to collect biometric data when absolutely necessary and when they can adequately allocate sources to maintain and secure the systems that utilize biometrics. Once the data is no longer servicing the original purpose of collection, it should be securely deleted.

Access control is another key component of a secure biometric authentication system. Access controls to sensitive biometric data should be built on principles of least privilege and on a need-to-know basis. To prevent repudiation, monitoring and logging services should be in use along with intrusion detection systems that work with heuristic signatures to detect anomalies and signs of data exfiltration.

The NIST 800-53 is a robust security framework that employs comprehensive strategies for securing information systems, including biometrics (NIST, 2020). Using a standardized framework allows auditors and security professionals to implement comparable security measures across industry verticals. The notable NIST controls that should be applies include:

- AC-3 Access Enforcement - Principle of least privilege to based on user roles
- SC-12 to SC-17 Cryptographic Protections - These numerous controls have specifications for end to end encryption that protects it from unauthorized access.
- SI-7 Software & Firmware Integrity - Requirements for system updates and patch management.

Combining the NIST 800-53 with the NIST SP 800-63-3 that offers identity assurance risk models (NIST, 2017) for biometric systems will allow protection using industry benchmarks.

Encryption of biometric data is required both in transit, and at rest. Storage of data in on-premise database servers or cloud servers must still be encrypted to ensure security as a compensatory measure for data breaches. FIPS 140-3 compliant encryption offers the highest level of data protection, and introduces significant hurdles in attempts for decryption.

Along with conventional encryption and authentication controls, organizations need to consider zero-identifier anonymization techniques for safeguarding biometric data. Removing direct identifiers from biometric data and replacing them with non-identifiable or pseudonymous tokens can minimize privacy violations in the event of a breach. Studies on zero-knowledge proofs and anonymized biometric data storage demonstrate that these systems reduce the potential for identity theft without a complete overhaul of existing biometric authentication systems (Fatime et al, 2024). In a similar manner, using cryptographic keys such as ones used for common cryptocurrency wallets is being explored as a means of reducing overall exposure by a decentralized system of authentication (Arjona et al, 2023)

As quantum technology evolves, it is theorized that widely used cryptographic methods such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) will no longer

be secure against the increased computing capacity offered by quantum computing. Organizations must begin to transition to post-quantum cryptography (PQC) in preparation for a future resistant infrastructure. NIST has recently released PQC standards that offer detailed recommendations for using quantum resistant encryption methods. Lattice-based cryptography is a strong contender in the PQC race and is expected to withstand the exponential computing powers of quantum computers (NIST, 2024a). Organizations can begin with preparing a roadmap for transitory states within intervals of 5 years. *Figure 2* below details a proposed roadmap for organizations to implement within the next 15 years to prepare for PQC.

Step #	**Term Length**	**Goal to Accomplish**
1	Short Term (0 - 5 Years)	Larger Key Sizes - Increasing the number of keys (AES 128 to AES 256) on current encryption modules helps provide a temporary buffer while long term solutions are sought and implemented (Akitra, 2025).
2	Mid Term (0 - 10 Years)	Implementing post quantum cryptography (PQC) based standards - NIST's updated Federal Information Processing Standard (FIPS) uses Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) for general encryption and digital signatures for ID authorization (NIST, 2024b).
3	Long Term (3 - 15 Years)	Quantum Key Distribution (QKD) - A developing method of cryptography, QKD uses quantum light signals to generate random quantum keys, which cannot be calculated or cracked (UK National Quantum Technologies, n.d.).

Figure 2: Sample Implementation Roadmap

Policy Recommendations to Safeguard Customer Biometric Data

Regulation is the backbone of biometric data protection as it becomes more widespread in use. Similarly, organizational controls are equally important for ensuring the data is secured within the authentication systems they are used. Because of the nature of biometric data being immutable, organizations must adopt a holistic approach to combine administrative, managerial, technical, and physical safeguards should they use biometric authentication. Audit and enforcement controls are also included to encourage organizations to be proactive in their biometric system compliance and set goals for improvements. Below are guiding controls in each of the aforementioned areas.

Regulatory Safeguards

Regulatory intervention plays a key role in national success in safeguarding biometric data. The following recommendations propose several guidelines as a blueprint for legislation and national enforcement. Although enforcing legislation is difficult and slow to implement, organizations should advocate for these measures and be proactive in how they approach and manage biometric data.

- Establish a Unified National Framework
    - Use informed consent akin to BIPA for enrollment
    - Aim for compliance with CCPA
    - Require explicit consent before collection
    - Mandate disclosure of purpose and retention period
    - Guarantee right to delete biometric data
    - Prevent fragmented state-by-state policy chaos through adoption of federal standardization
- Enforce Stronger Breach Notification Laws
    - Require organizations to disclose biometric breaches within defined timelines
    - Mandate identity protection services and cancelability support post-breach
- Create Biometric Data Protection Standards
    - Define and enforce technical standards similar to PCI-DSS for credit cards
    - Oversight may be managed by a federal body or independent consortium
- Promote R&D for Privacy-Preserving Biometrics
    - Fund research in homomorphic encryption, zero-knowledge proofs, and secure enclaves (Thorve et al., 2023)
    - Support emerging areas like EEG biometrics and behavioral data protection
- Audit and Enforce
    - Equip FTC and other regulators with power to conduct biometric system audits and issue fines

    - Model enforcement of enforcement of General Data Protection Requirements' (GDPR) fine structure to deter non-compliance
- Create a framework for repudiation for users who have had their biometric data compromised and used in identity theft exceeding a defined monetary threshold
    - May include creating a governing body that oversees this agency akin to the Consumer Financial Protection Bureau (CFBP)

Administrative Safeguards

Although organizations can follow some legislative suggestions internally, administrative safeguards are the foundation for organizational biometric data protection. These safeguards focus on establishing accountability and create privacy awareness within operations. By implementing these safeguards, organizations can minimize compliance risks in the future as society moves towards being passwordless.

- Appoint Chief Privacy or Biometric Data Officer to oversee policy creation and adherence within the organization
- Enforce mandatory training programs focal on privacy-by-design for biometric data handlers
    - Hardware and software training maintenance
    - Best practices for data protection within the organization (on-prem or cloud)
- Maintain and enforce an explicit data lifecycle policy that defines storage, user, and deletion conditions for biometric records
- Integrate biometric data into existing data classification schemes and assign them with the highest sensitivity in risk policy appetite documentation

Managerial Safeguards

Managerial safeguards emphasize oversight and strategic integration of biometric risk into an organization's existing risk management process. These safeguards help to ensure that controls are given the same level of attention as other critical assets through contract enforcement, asset tracking, and clearly defined risk thresholds.

- Conduct annual biometric risk assessments utilizing risk management and related organizational risk registers
- Define a risk appetite statement that adequately describes biometric-specific thresholds for exposure and loss with the aim to minimize both of these conditions
- Identify biometric assets and track their life cycles
- Vendor contracts should require zero-knowledge proof compliance when applicable, breach notification timelines, and enforceable audit rights for business partners

Technical Safeguards

These safeguards form the infrastructure for biometric data protection at the source and encompasses encryption and architectural design decisions. These controls aim to maintain

confidentiality, integrity, and availability of biometric systems in the face of quantum computing and Internet of Things (IoT) vulnerabilities.

- Implement post-quantum cryptography in preparation for future threats
- Require multimodal biometric authentication where feasible to prevent single point of failure
- Ensure cancelable biometric templates are used
- If blockchain or decentralized storage is used, ensure zero-knowledge proof capabilities exist
- Follow national or international standards to build interoperability into systems to prevent lock-in on legacy systems
- Implement zero-trust architecture to protect and monitor IoT devices

Physical Safeguards

Physical safeguards are critical to ensure that hardware requirements and environments where biometric readers and processors are protected from tampering, theft, or unauthorized access. These are key to keeping biometric systems secure in decentralized environments where exposure to physical threat actors are heightened.

- Secure physical biometric authentication devices with tamper-proof hardware and monitored physical access control through use of cameras or other detection mechanisms
- Restrict access to biometric processing servers to authorized personnel only and utilize defense-in-depth to secure these areas
- Provide physical security to IoT device deployment where used for edge computing

These layered safeguards form a comprehensive framework for biometric data protection for consumers to mitigate the amount of harm they may face as biometric usage increases. Consumer-centric biometric security is not solely reliant on the latest and greatest technology, but also on the underlying governance mechanisms both on a national and organizational level. If organizations are not capable of providing adequate security for biometric systems, it is recommended to not employ them.

Conclusion

Biometric authentication provides a transformative approach to digital security, however, it comes with complex and far-reaching implications on consumers. The high cost of secure implementation and maintenance raises concerns about long-term privacy of consumers and the viability of this technology as a whole.

Capabilities in biometrics are rapidly improving, such as new modalities found in EEG and palm vein recognition entering the mainstream. However, the risks associated with biometric systems that include immutable data breaches, deepfake attacks for less robust systems, and algorithmic bias may outpace even the most proactive organization’s preparedness. Many institutions lack the infrastructure, training, resources, or internal policies to adequately deploy

and maintain biometric systems responsibly. At the same time, consumers are largely unaware of how their biometric data is collected, used, stored, or repurposed with or without their consent.

To aid in addressing organizational accountability for consumers, we propose a multi-layered, future-facing response that encompasses administrative, technical, and physical safeguards alongside national legislative action. The future of biometric authentication does not rely alone on technology, but on governance both inside and outside of the organization. As we move towards a passwordless future, secure, revocable, and privacy-preserving systems will be essential to protect consumers. Without meaningful action by organizations or legislative bodies, biometric authentication may enact more harm than good.

References

ACLU Illinois. (2021, April 26). *Biometric Information Privacy Act (BIPA)*. ACLU of Illinois. https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa

Akitra. (2025). *Medium*. Medium. https://medium.com/@akitrablog/the-invisible-threat-how-quantum-computing-could-break-todays-encryption-888e3ea99cf3.

Allano, L., Dorizzi, B., & Garcia-Salicetti, S. (2010). Tuning cost and performance in multi-biometric systems: A novel and consistent view of fusion strategies based on the Sequential Probability Ratio Test (SPRT). *Pattern Recognition Letters*, *31*(9), 884–890. https://doi.org/10.1016/j.patrec.2010.01.028

Amine Hmani, M., Petrovska-Delacretaz, D., & Dorizzi, B. (2024). Revocable Crypto-Biometric Key Regeneration Using Face Biometrics, Fuzzy Commitment, and a Cohort Bit Selection Process. *Biometrics and Cryptography*. https://doi.org/10.5772/intechopen.1003710

Arjona, R., López-González, P., Román, R., & Baturone, I. (2023). Post-Quantum Biometric Authentication Based on Homomorphic Encryption and Classic McEliece. *Applied Sciences*, *13*(2), 757–757. https://doi.org/10.3390/app13020757

Ayyar, K. (2018, September 26). *India's Supreme Court Upholds Biometric ID System*. Time. https://time.com/5388257/india-aadhaar-biometric-identification/

Beyrouthy, T., Mostafa, N., Roshdy, A., Karar, A. S., & Samer Alkork. (2024). Review of EEG-Based Biometrics in 5G-IoT: Current Trends and Future Prospects. *Applied Sciences*, *14*(2), 534–534. https://doi.org/10.3390/app14020534

Birch, I., Birch, M., & Asgeirsdottir, N. (2020). The identification of individuals by observational gait analysis using closed circuit television footage: Comparing the ability

and confidence of experienced and non-experienced analysts. *Science & Justice*, *60*(1), 79–85. https://doi.org/10.1016/j.scijus.2019.10.002

Bolgar, C. (2025, February 19). *Microsoft's Majorana 1 chip carves new path for quantum computing - Source*. Microsoft. https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/

Borak, M. (2025, January 3). *2025 deepfake threat predictions from biometrics, cybersecurity insiders*. Biometric Update | Biometrics News, Companies and Explainers; BiometricUpdate.com. https://www.biometricupdate.com/202501/2025-deepfake-threat-predictions-from-biometrics-cybersecurity-insiders

Burt, C. (2023, June 21). *As iris biometrics takes on greater prominence, Neurotechnology touts NIST results*. Biometric Update | Biometrics News, Companies and Explainers; BiometricUpdate.com. https://www.biometricupdate.com/202306/as-iris-biometrics-takes-on-greater-prominence-neurotechnology-touts-nist-results

The Business Case for Biometric Authentication. (2018). *Goode Intelligence*. https://www.goodeintelligence.com/wp-content/uploads/2018/09/Goode-Intelligence-White-Paper-The-Business-Case-for-Biometric-Authentication.pdf

CardLogix. (n.d.). *Biometric Iris Cameras, Scanners, Mobile Devices, Tablets and Kiosks*. Www.cardlogix.com. Retrieved April 18, 2025, from https://www.cardlogix.com/product-category/biometrics/iris-cameras/

Chen, H., & Magramo, K. (2024, February 4). *Finance worker pays out $25 million after video call with deepfake "chief financial officer."* CNN. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

Choi, T. (2022, May 9). *Biometric template explainer | Biometric Update*. Www.biometricupdate.com. https://www.biometricupdate.com/202205/biometric-template-explainer

Clark, M. (2017, September 11). *Biometric Devices: Cost, Types and Comparative Analysis*. Bayometric; Bayometric. https://www.bayometric.com/biometric-devices-cost/

DigiCert. (2023, November 18). *DigiCert Global Study: Preparing for a Safe Post-Quantum Computing Future*. Digicert.com. https://www.digicert.com/news/digicert-global-study-preparing-for-a-safe-post-quantum-computing-future

Dike-Anyiam, B., & Rehmani, Q. (2006). Biometric vs. Password Authentication: A User's Perspective. *Journal of Information Warfare*, *5*(1), 33–45. https://www.jstor.org/stable/26502888

ETtech. (2023, October 31). Aadhaar data leak | Personal data of 81.5 crore Indians on sale on dark web: report. *The Economic Times*. https://economictimes.indiatimes.com/tech/technology/aadhar-data-leak-personal-data-of-81-5-crore-indians-on-sale-on-dark-web-report/articleshow/104856898.cms

Fatima, M., Banu, R., Shojae Chaeikar, S., & Khanian Najafabadi, M. (2024). Biometric Systems in Focus: A Review of Methods, Challenges, and Future Directions. *2024 International Conference on Intelligent Computing and next Generation Networks (ICNGN)*, 01–07. https://doi.org/10.1109/icngn63705.2024.10871800

FDC. (2025, January 30). *Physical Security Attack Examples: 7 Ways to Mitigate - FDC*. FDC Inc. https://www.fdc.com/physical-security-attack-examples

Fruhlinger, J. (2020). *The OPM hack explained: Bad security practices meet China's Captain America*. CSO Online. https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

FTC. (2023, May 18). *FTC Warns About Misuses of Biometric Information and Harm to Consumers*. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers

Government of India. (2023). *GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY LOK SABHA*. https://uidai.gov.in/images/ISSUE_OF_AADHAAR_CARD_English.pdf

Greenberg, A. (2015, September 23). *OPM Now Admits 5.6m Feds' Fingerprints Were Stolen by Hackers*. Wired. https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers

Haider, S. A., Ashraf, S., Larik, R. M., Husain, N., Muqeet, H. A., Humayun, U., Yahya, A., Arfeen, Z. A., & Khan, M. F. (2023). An Improved Multimodal Biometric Identification System Employing Score-Level Fuzzification of Finger Texture and Finger Vein Biometrics. *Sensors*, *23*(24), 9706–9706. https://doi.org/10.3390/s23249706

Irshad, A., Usman, M., Chaudhry, S. A., Bashir, A. K., Jolfaei, A., & Srivastava, G. (2020). Fuzzy-in-the-Loop-Driven Low-Cost and Secure Biometric User Access to Server. *IEEE Transactions on Reliability*, 1–12. https://doi.org/10.1109/tr.2020.3021794

James, L. (2025, February 28). *Face-swapping: Why you can't trust a video call – and how scammers are taking advantage*. The Independent. https://www.the-independent.com/tech/deepfake-scam-face-swap-fraud-ai-b2706722.html

Koehler, J. J., & Liu, S. (2020). Fingerprint error rate on close non-matches. *Journal of Forensic Sciences*, *66*(1). https://doi.org/10.1111/1556-4029.14580

Markets and Markets. (2023). *Biometric System Market by Authentication Type, OfferingType, Type, Vertical | COVID-19 Impact Analysis | MarketsandMarkets™*. Www.marketsandmarkets.com. https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html

McGowran, L. (2022, August 19). *Quantum apocalypse: Experts warn of 'store now, decrypt later' hacks*. Silicon Republic. Retrieved April 14, 2025, from https://www.siliconrepublic.com/enterprise/quantum-apocalypse-store-now-decrypt-later-encryption

McKenna, S., Lead, J., & Sarage. (2015). *Biometric Analytics Cost Estimating*. https://www.iceaaonline.com/wp-content/uploads/2015/06/MM09-Paper-Sarage-Biometric-Analytics.pptx.pdf

Meden, B., Rot, P., Terhorst, P., Damer, N., Kuijper, A., Scheirer, W. J., Ross, A., Peer, P., & Struc, V. (2021). Privacy–Enhancing Face Biometrics: A Comprehensive Survey. *IEEE Transactions on Information Forensics and Security*, *16*, 4147–4183. https://doi.org/10.1109/tifs.2021.3096024

Min-Allah, N., Nagy, N., Aljabri, M., Alkharraa, M., Alqahtani, M., Alghamdi, D., Sabri, R., & Alshaikh, R. (2022). Quantum Image Steganography Schemes for Data Hiding: A Survey. *Applied Sciences*, *12*(20), 10294. https://doi.org/10.3390/app122010294

Ngugi, N., Kamis, N., & Tremaine, N. (2011). Intention to Use Biometric Systems. *E-Service Journal*, *7*(3), 20–20. https://doi.org/10.2979/eservicej.7.3.20

NIST. (2017). *NIST SP 800-63 Digital Identity Guidelines*. Nist.gov. https://pages.nist.gov/800-63-3

NIST. (2024a, August 13). *NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST*. NIST. http://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

NIST. (2024b, August 13). *Post-Quantum Cryptography | CSRC | CSRC*. CSRC | NIST. https://csrc.nist.gov/projects/post-quantum-cryptography

NIST. (2025, March 18). *Quantum Computing Explained | NIST*. NIST. https://www.nist.gov/quantum-information-science/quantum-computing-explained

OVIC. (2019). *Biometrics and Privacy - Issues and Challenges*. Office of the Victorian Information Commissioner. https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges

Raposo, V. L. (2023). When facial recognition does not “recognise”: erroneous identifications and resulting liabilities. *AI & SOCIETY*, *39*. https://doi.org/10.1007/s00146-023-01634-z

Singh, S., & Kant, C. (2017). *A Novel Approach to Secure Biometric Template with Steganography*. International Journal of Advanced Research in Computer Science. https://www.proquest.com/docview/1912631259?_oafollow=false&accountid=9902&pq-origsite=primo&sourcetype=Scholarly%20Journals

Sinha, A., Dutta, U., Demir, O. M., De Silva, K., Ellis, H., Belford, S., Ogden, M., Li, M., Morgan, H. P., Shah, A. M., Chiribiri, A., Webb, A. J., Marber, M., Rahman, H., & Perera, D. (2024). Rethinking False Positive Exercise Electrocardiographic Stress Tests

by Assessing Coronary Microvascular Function. *Journal of the American College of Cardiology*, *83*(2), 291–299. https://doi.org/10.1016/j.jacc.2023.10.034

Sjouwerman, S. (2024, July 23). *How a North Korean Fake IT Worker Tried to Infiltrate Us*. Blog.knowbe4.com. https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

Thorve, A., Shirole, M., Jain, P., Santhumayor, C., & Sarode, S. (2023). *Decentralized Identity Management Using Blockchain | IEEE Conference Publication | IEEE Xplore*. Ieeexplore.ieee.org. https://ieeexplore.ieee.org/document/10074477

Total Security Solutions. (2021, August 13). *Mantrap vs. Secure Vestibule for Corporate Offices and Professional Buildings - Total Security Solutions*. Tssbulletproof.com. https://www.tssbulletproof.com/blog/mantrap-secure-vestibule-corporate-offices-and-professional-buildings

UK National Quantum Technologies. (n.d.). *Quantum-Safe Secure Communications*. https://uknqt.ukri.org/wp-content/uploads/2021/10/Quantum-Safe-Secure-Communications.pdf

Walters, W., & Vanderlip, D. (2015). Electronic Passports. In M. B. Salter (Ed.), *Making Things International 1: Circuits and Motion (pp. 3–17)*. University of Minnesota Press. http://www.jstor.org/stable/10.5749/j.ctt14jxw02.4

Woodward, J. D. (2007). The Law and the Use of Biometrics. *Springer EBooks*, 357–379. https://doi.org/10.1007/978-0-387-71041-9_18

Zhou, L., Blackley, S. V., Kowalski, L., Doan, R., Acker, W. W., Landman, A. B., Kontrient, E., Mack, D., Meteer, M., Bates, D. W., & Goss, F. R. (2018). Analysis of Errors in Dictated Clinical Documents Assisted by Speech Recognition Software and

Professional Transcriptionists. *JAMA Network Open*, *1*(3), e180530.

https://doi.org/10.1001/jamanetworkopen.2018.0530