cognizancejournal.com
Mary Pauline D. Calungsod *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.5, Issue.9, September 2025, pg. 295-302
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 5.183**
**Index Copernicus Value (ICV) = 92.57**

# Iris Scanning: An Evaluation of Data Privacy and Security in World App's Biometric System

**Mary Pauline D. Calungsod[1]; Ronald O. Ajusan[2]; Kimberly G. Eledia[3]; Matthew G. Hernandez[4]; Pops V. Madriaga[5]**

Electrical and Allied Department, Technological University of the Philippines – Taguig Campus, Taguig City, Philippines
[1] marypauline.calungsod@tup.edu.ph; [2] ronald.ajusan@tup.edu.ph; [3] kimberly.eledia@tup.edu.ph; [4] matthew.hernandez@tup.edu.ph; [5] pops_madriaga@tup.edu.ph

**DOI: 10.47760/cognizance.2025.v05i09.023**

**Abstract: The increasing use of modern biometrics technology, such as Iris Scanning, is strong evidence of our generation leaning towards innovation and trust in modern technology. The World App by Worldcoin is a prime example of this. This app has been gaining recognition locally for offering accessible and safe access to financial services. Although the new generation is quick to adapt to new technology, numerous debates are emerging online about whether this app can truly deliver on its promises to users and whether it can effectively uphold data security, which is increasingly crucial in modern technology. Nowadays, news about data security has been flooding the internet due to the numerous victims of online fraud. This study will examine whether the World App can protect its users' data, which it has collected through its iris scanning device, known as the "Orb". This will cover related issues, such as identity theft, spoofing, and data breaches. Iris patterns are considered unique data for each person, which poses a permanent risk to millions of individuals; as a result, it could lead to data misuse if compromised. Moreover, this encompasses ethical and legal issues, such as data transparency, user consent, and legal regulations like the General Data Protection Regulation (GDPR). This will also discuss the importance of maintaining security protocols and handling sensitive biometric data in building trust with users. The imposing threats it would bring, although iris scanning improves security, reduces fraud, and accelerates digital verification, are undeniable. This study examines how World App's biometric iris scanning system addresses user privacy and security concerns by considering the risks and opportunities associated with iris scanning on financial digital platforms.**

**Keywords: Worldcoin, World App, Iris Scanning, Data Breaches, Biometrics Security, Digital Verification, Orb, Data Security, General Data Protection Regulation (GDPR), Spoofing, Identity Theft**

## I. INTRODUCTION

People are asking for simpler ways to complete daily tasks, and our technology needs to keep up with their demands, especially in the financial sector. In response, biometric authentication is one of the most widely used developments in digital security. Everywhere you go, biometrics can be seen, whether in government agencies, large businesses, or even on busy streets. Iris scanning is a type of biometric authentication that is often regarded as one of the most effective methods for verifying identity. It helps protect privacy and improve security since the data cannot be copied. [1].

Nowadays, the World app has been gaining local attention for offering iris scanning to its users. They integrated iris scanning through a device they called an "Orb." Essentially, users need to register an account on

*©2025, Cognizance Journal, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden, All Rights Reserved* 

cognizancejournal.com
Mary Pauline D. Calungsod *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.5, Issue.9, September 2025, pg. 295-302
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 5.183**
**Index Copernicus Value (ICV) = 92.57**

their device and select a location to complete the final step, which is the scanning process. This app was designed to serve as a secure storage for a digital ID and facilitate the exchange of digital assets. This app allows its users to access their assets online, verify that they are not bots, and use tokens called "Worldcoin" where available [2].

The app offers financial rewards to users who invite others, which could draw many people to try it without fully understanding what information they are sharing. This raises significant concerns about user privacy and security. The data from the iris scan can be especially alluring to attackers since it is impossible to manipulate. The ethical standards should be appropriately monitored by collecting biometric data in a transparent and informed manner through consent. In line with this, the standards should meet GDPR requirements to monitor security threats and protect user data.

## II. METHODOLOGY

This part of the study will describe the company's data handling practices in terms of privacy and security, utilizing iris scanning technology. This will cover the collection of iris scans, identify risks, apply laws and policies, and consider the likelihood and impact of such risks.

### *A. Data Collection of Iris Scanning*

The first step in the methodology will demonstrate how biometric data is processed and stored on the World App system. With the use of eye recognition technology, the researchers will analyze how iris scans are collected, used, stored, and deleted, in relation to identifying security and privacy issues [10],[11].

The data gathering starts with using World App's "Orb" tool to capture an image of the eye. The raw data is then made into an iris template that is hidden. It is important to tell the difference between encrypted templates and raw pictures because encrypted templates have unique identifiers that are very important. However, raw pictures still need strong security measures [12]. Processed data is either kept locally or sent to central servers, where encryption technologies like TLS 1.3 are used for transport and AES-256 is used for storage to protect against cyberattacks and unauthorized access. [13].

At this stage of creating storage, the pros and cons of both local device storage (which lowers risk) and centralized cloud storage (which makes it easier to scale but raises risk) are also looked at. The study also examines safe routes, data minimization, and anonymization methods for sharing data with third parties that comply with international privacy laws [11],[14].

The expected outputs include a data flow diagram that maps the journey of iris data, an inventory of data types and encryption measures, and an identification of potential vulnerabilities. This foundational assessment prepares for evaluating threats, compliance, and user trust in World App's biometric system [10],[15].

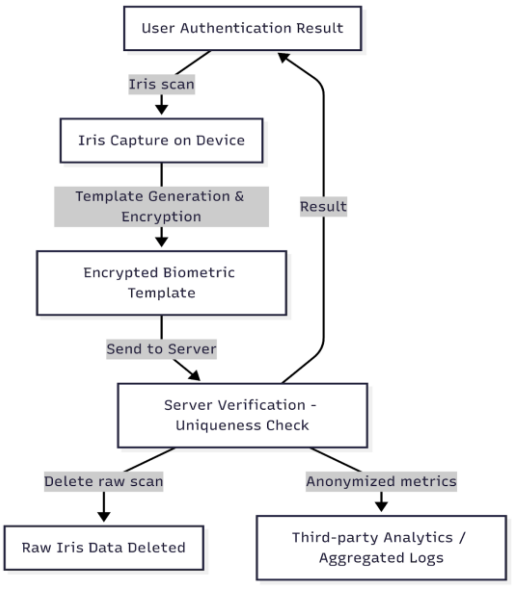


*Figure 1. Data flow diagram of Iris Data*

*©2025, Cognizance Journal, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden, All Rights Reserved* 

cognizancejournal.com
Mary Pauline D. Calungsod *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.5, Issue.9, September 2025, pg. 295-302
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 5.183**
**Index Copernicus Value (ICV) = 92.57**

This diagram illustrates the process of capturing an individual's iris, converting it into an encrypted template, sending it for verification, and then deleting the original image. To protect privacy, anonymized proofs are kept on the blockchain.

| Data Type | Storage Location | Encryption/Protection | Notes |
|---|---|---|---|
| Raw iris scan | Device memory temporary | Encrypted for transmission; deleted after scan | Never stored permanently |
| Biometric template / hash | Temporary server memory | Used for verification; deleted after use | Not stored permanently |
| Verification proof / uniqueness | Temporary server memory | Cryptographically secured; cannot reveal raw data | Public proof of uniqueness only |
| User ID / Account Info | Server Database (temporary) | Encrypted; access-controlled | Used for verification only |
| Authentication logs / timestamps | Server logs | Access-controlled; TLS for transmission | Anonymized / aggregated |
| Anonymized metrics / analytics | Analytics servers | Aggregated; anonymized; TLS in transit | Anonymized / aggregated |

*Figure 2. Different Data Types and Encryption Methods*

The table shows the different data types handled by the World App and stores them in different places. To safeguard user privacy and security, each category of data is encrypted or otherwise securely sealed.

| System Component | Potential Vulnerability | Risk Level | Mitigation / Notes |
|---|---|---|---|
| Iris capture (User device) | Spoofing attack (fake iris image) | High | Use liveness detection; device-level encryption |
| Data transmission | Interception / Man-in-the-middle attack | Medium | TLS 1.3 encryption; secure channels only |
| Temporary server memory | Unauthorized access to templates during verification | High | Access controls; delete template immediately after use |
| Blockchain verification proof | Linking anonymized proof to real identity (re-identification) | Low | Only store hashed proofs; no PII on blockchain |
| Authentication logs | Insider threat / log tampering | Medium | Encrypt logs; limit access; regular audits |
| Analytics / metrics | Aggregation could leak user patterns | Low | Only anonymized, aggregated data; no raw templates |
| User ID / account info | Exposure during verification | Medium | Use temporary IDs; delete after verification |
| Device metadata | Device tracking or location inference | Low | Anonymize metadata before storage |

*Figure 3. Assessing Vulnerabilities*

This illustration maps out where data could potentially be accessed and the risks tied to each point, revealing privacy and security concerns within the World App's iris-scanning system.

### *B. Risk Assessment of Iris Scanning*

In the second phase, researchers categorize and measure the risks connected to the iris scanning function. Since iris data is permanent, it becomes an appealing target for cybercriminals, making it essential to recognize these risks to grasp the technology's challenges and advantages fully.

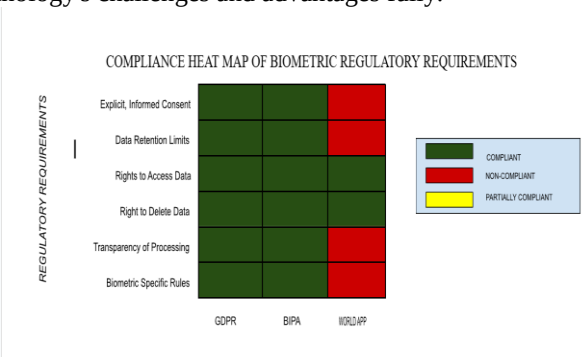


*Figure 4. Heat Map for Risk Assessment*

*©2025, Cognizance Journal, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden, All Rights Reserved* 

cognizancejournal.com
Mary Pauline D. Calungsod *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.5, Issue.9, September 2025, pg. 295-302
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 5.183**
**Index Copernicus Value (ICV) = 92.57**

To carry out this stage effectively, researchers group each detected threat into technical, legal, and ethical categories. This procedure will help identify vulnerabilities in the biometric system, particularly in areas such as iris data security and transparency, which could be heavily exploited during a data breach [3][4][5]. Through this process, both users and researchers obtain a clearer understanding of how the World App's iris-scanning feature works.

### *C. Evaluation of Iris Scanning from a Legal and Policy Perspective*

During this phase, the assessment will verify whether the World app's biometric data collection system complies with current legal and regulatory requirements. The evaluation compares the app's documented practices to the standards set by frameworks such as the General Data Protection Regulation (GDPR) and Illinois' Biometric Information Privacy Act (BIPA) [8],[9]. It addresses data processing and use, retention periods, user permissions, and options for access and deletion. BIPA mandates rigorous consent and protection procedures for biometric information [6]. Since biometric details qualify as personal data under the GDPR, users must provide explicit, informed consent [9].

| Requirement | World App Compliance |
|---|---|
| Informed Consent | Exists but needs confirmation for clarity and documentation |
| Data Retention Limits | Retention schedule disclosed; automatic deletion not fully verified. |
| Right to Access Data | Users can request data, but the response process requires review. |
| Right to Delete Data | Deletion rights available; timeliness of execution unclear. |
| Process Transparency | Public privacy policy provided, but ongoing updates and details should be checked. |
| Biometric Encryption | Encryption in place; breach-notification plan needs further validation. |

*Figure 5: World App vs. Important Regulations Compliance Checklist*

This process examines the benefits and drawbacks of the World App, focusing on issues such as the legitimacy of informed consent, data reduction and limitation, and users' rights to access or remove their personal information.

### *D. Impact and Likelihood Risk Assessment*

This stage looks at both technical and social aspects to understand the full impact of World App's iris-scanning system. It considers factors such as the strength of the encryption and whether the Orb hardware could be misused. Each risk is rated as Low, Medium, High, or Critical, depending on how likely it is to happen and how severe its effects on society could be. Meanwhile, impact shows the potential harm of storing permanent biometric data along with the regulatory consequences it may trigger.

Since iris patterns are considered sensitive data, recent data demonstrate weaknesses in data breaches and loss of public trust, which are seen as the most pressing issues, and both scored strongly on the axis [5]. Other risks, ranging from medium to high, include device exploitation, privacy concerns, and failure to comply with regulatory frameworks.

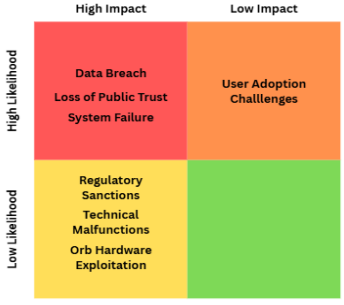


*Figure 6. Risk Matrix Quadrant*

*©2025, Cognizance Journal, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden, All Rights Reserved* 

cognizancejournal.com
Mary Pauline D. Calungsod *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.5, Issue.9, September 2025, pg. 295-302
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 5.183**
**Index Copernicus Value (ICV) = 92.57**

Evaluating every risk in terms of its probability and the amount of harm that it might produce, it becomes more comfortable to resolve the problems successfully. By strengthening the privacy infrastructure through the application of zero-knowledge proofs, enhancing the hardware used, and ensuring that biometric information is stored correctly, the risks can be minimized. The company should transparently explain how the data collected from users is handled and comply with relevant laws and policies to continue conducting business. With this method, identifying and addressing risks will be easier.

## III. RESULTS AND DISCUSSION

This section shows the results and discussion of the study based on the methodology presented concerning data collection, risk assessment, compliance with legal and policies, and the likelihood and impact of risks. This part also highlights the growing global population of World App users, which raises concerns about privacy and data security.

### *A. Data Handling and Vulnerability Assessment'*

The description of the World App's data flow makes clear the risks associated with iris scans as well as how the security measures implemented to the data flow are handled given that an iris scan has been obtained to the point of being kept. Hardware records indicate that the system is configured to encrypt its templates using a robust encryption program, thereby erasing the original images. TLS 1.3 provides security to data sent over networks, and AES-256 encryption is used to secure data stored on central servers. It is also the system that analyzes with zero-knowledge proofs and Secure Multi-Party Computation to confirm users without revealing their biometric information [4].

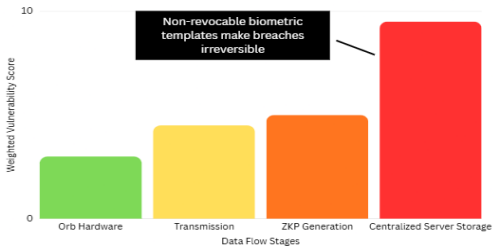


*Figure 7. Vulnerability Score Comparison*

The graph underscores the fact that encrypted iris templates should not be kept in a central location due to a significant vulnerability. Even with strong encryption, keeping sensitive biometric data together increases the risk of targeted attacks, which could result in permanent exposure of personal information [5]. The lack of independent or third-party verification also raises doubts about the effectiveness of the security measures and whether the company's claims can be trusted [4].

### *B. Model Performance: Legal and Policy Compliance*

The results reveal a clear pattern of non-compliance and regulatory backlash worldwide, despite international legal frameworks such as the Biometric Information Privacy Act (BIPA) and the General Data Protection Regulation (GDPR).

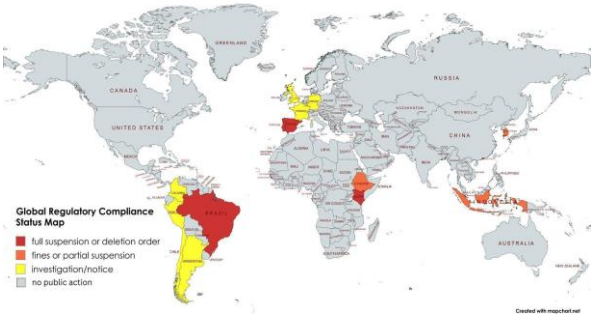


*Figure 8. Global Regulatory Compliance Status Map*

*©2025, Cognizance Journal, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden, All Rights Reserved* 

cognizancejournal.com
Mary Pauline D. Calungsod *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.5, Issue.9, September 2025, pg. 295-302
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 5.183**
**Index Copernicus Value (ICV) = 92.57**

As shown in the global map above, many countries have already halted World App's operations, including Kenya, Hong Kong, Portugal, and Spain, due to privacy concerns. Key rulings underscore the severity of these issues: South Korea imposed fines for failing to inform users about data handling and overseas transfers properly; Kenya ordered the deletion of all biometric data for breaching its Data Protection Act; and Indonesia raised alarms about the company's legal registration and unauthorized activities [14].

These actions go against the GDPR's main requirements for lawfulness, transparency, and user control [3]. In addition, by offering cryptocurrency (WLD) in exchange for biometric data, the company makes it harder to claim that users are giving genuine, informed consent. This raises questions about whether its data collection meets strict international standards.

### *C. Impact and Likelihood Risk Validation*

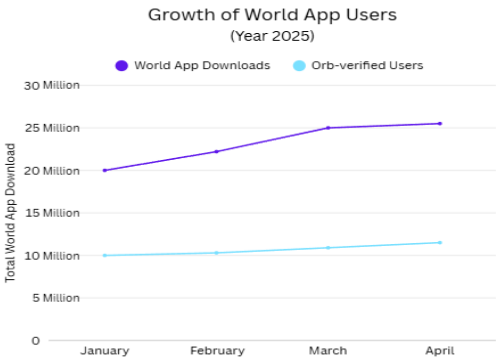


*Figure 9. World App Downloads vs. Verified Users*

The graph indicates that the World App now boasts over 10 million Orb-verified users and has surpassed 25 million downloads worldwide. As the user base grows quickly, the risks of major failures increase [7].

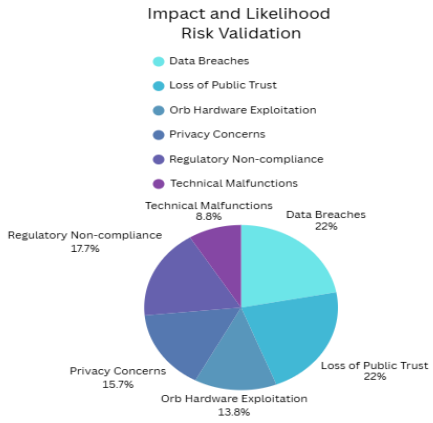


*Figure 10. Impact and Likelihood Risk Validation Chart*

As shown in the chart, the risks reportedly associated with the World App include regulatory non-compliance, technical malfunctions, privacy concerns, hardware exploitation, and loss of public trust, with these being the top concerns [8]. As the data undergoes a complex process, it creates several weak spots. Among the users, people who struggle financially often resort to the incentives offered by the company in return for their eye scan [4]. Although the company emphasizes that biometric information is not stored in a single central location, the risk of a data breach remains a pressing concern. Such a single repository is an appealing target for hackers and other cybercriminals [5]. To counter this vulnerability, the company must urgently strengthen both its technical defenses and its policy compliance measures.

*©2025, Cognizance Journal, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden, All Rights Reserved* 

## IV. CONCLUSIONS

The evaluation shows iris-scanning technology holds great promise for enhancing digital financial verification, provided it is used responsibly and subject to strict security regulations. When utilized properly, it also reduces fraud and can be used to quickly and reliably authenticate individuals.

However, the analysis points up significant flaws. While Worldcoin stated that they do not rely on a single, centralized database to store extremely sensitive biometric data, there are still concerns about long-term security and managing derived iris codes. Even though the business claims to have adopted the most recent encryption protocols—TLS 1.3 for data transmission and AES-256 for data storage—no system can guarantee complete security. Critical issues, such as data breaches, failure to comply with legal frameworks, and the inability to maintain data visibility, are also addressed by the technique. The above issues highlight the challenges that biometric technology poses, as any single error or misuse of data can lead to irreversible damage.

Regardless of these reservations, the iris scanning has immense potential to increase the level of financial digital verification when used and implemented in the right way. The researchers have concluded that the importance of rigid security and legal conditions for all technological advancements is affirmed. The user would only have full confidence in the biometric system if it provided transparency, compliance, and security, ensuring that it would never compromise identity.

## ACKNOWLEDGEMENT

We sincerely thank everyone who helped make this research possible. First and foremost, to God who guided and gave us valuable knowledge to complete this study. We are also grateful to our adviser for her valuable insights, feedback, and continuous guidance throughout the study. We are especially thankful to our classmates who provided us with advice during the development and evaluation phases, and those who helped us with their insights. Finally, to our parents for their unwavering support, be it in terms of emotional and financial aspects, which allowed us to accomplish this project.

# REFERENCES

1. Iris ID. (2023, November 3). Using iris biometric technology enhances security and protects privacy. Iris ID. https://www.irisid.com/using-iris-biometric-technology-enhances-security-and-protects-privacy/
2. Tools for Humanity. (n.d.). World App provides simple and easy access to World Network. World. Retrieved September 15, 2025, from https://world.org/world-app
3. Baker, S. (2019). The European Union's General Data Protection Regulation: How it represents a paradigm shift in personal data protection. Information & Communications Technology Law, 28(1), 43–58. https://doi.org/10.1080/1097198X.2019.1569186
4. Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. AI & Society, 37(1), 167–175. https://pubmed.ncbi.nlm.nih.gov/33867693/
5. Kindt, E. J. (2020). The risks involved upon the use of biometric data and biometric systems. In privacy and data protection issues of biometric applications (pp. 275–401). Springer. https://link.springer.com/chapter/10.1007/978-94-007-7522-0_4
6. Biometric Information Privacy Act (BIPA). (2025, March 4). Almeida Law Group | Class Action, Data Breach & Consumer Law. https://www.almeidalawgroup.com/data-security-and-privacy/illinois-biometric-information-privacy-act/
7. Watson, R. (2025, January 10). Sam Altman's World project passes 10 million human verifications. The Block. https://www.theblock.co/post/334042/sam-altmans-world-project-passes-10-million-human-verifications
8. McConvey, J. R. (2024, December 19). World does not comply with GDPR, says German regulator. Biometric Update | Biometrics News, Companies and Explainers; BiometricUpdate.com. https://www.biometricupdate.com/202412/world-does-not-comply-with-gdpr-says-german-regulator
9. Compliance Brief: Data Minimization under GDPR, CCPA and other Privacy Laws | TrustArc. (2024). TrustArc. https://trustarc.com/resource/data-minimization-gdpr-ccpa-privacy-laws/
10. Worldcoin. (2023a). Privacy at Worldcoin: A technical deep dive - Part I. Retrieved from https://world.org/blog/developers/privacy-deep-dive
11. ISO/IEC 29100:2011. (2021). Information technology – Security techniques – Privacy framework. International Organization for Standardization. Retrieved from https://www.iso.org/standard/45123.html
12. Worldcoin. (2023b). Iris recognition inference system. Retrieved from https://world.org/blog/engineering/iris-recognition-inference-system

*©2025, Cognizance Journal, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden, All Rights Reserved* 

**13.** Worldcoin. (2023c). A look inside Worldcoin's biometric imaging device. Retrieved from https://world.org/blog/engineering/opening-orb-look-inside-worldcoin-biometric-imaging-device
**14.** Noor Al-Sibai. (2024, August 19). More Than a Dozen Countries Now Investigating Sam Altman's Dubious Eye-Scanning Scheme. Futurism. https://futurism.com/the-byte/sam-altman-worldcoin-investigation
**15.** Worldcoin. (2024). Worldcoin orb privacy and security audit report. Retrieved from https://world.org/blog/world/worldcoin-orb-privacy-security-audit-report

*©2025, Cognizance Journal, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden, All Rights Reserved* 