STAND DD54
hr technologies
London UK 2025

SYNEL™

MAKE
EVERY MINUTE COUNT™

TECH-SAVVY OR TOO INTRUSIVE? THE DEBATE OVER BIOMETRICS IN BUSINESS

WHITEPAPER

WWW.SYNEL.CO.UK
WORKFORCE MANAGEMENT SOLUTIONS

BIOMETRICS IN BUSINESS

As with most things in life, there is a time and place for using people's biometric uniqueness to identify them. There are a number of differing ways to do this, from measuring gait while people walk to using their fingerprints or facial features.

The deeper lying issues are in determining when to employ such methods, and how to do so in the most appropriate and least intrusive way.

The ~~corporate~~ day-to-day use cases for identifying individuals are myriad. You may be asked to use a PIN code to authorise a sales transaction, or present an access card to enter a building, or use your face to unlock your phone. Our day-to-day interactions with identity management are endless.

In a recent case, the ICO ordered Serco to stop using Facial Recognition and Fingerprint Recognition technology as part of the Time and Attendance solution. They were using the technology to ascertain when employees were clocking in, or out, of shifts.

The ICO found that Serco had failed to show the necessity and proportionality of using the technology, as opposed to less intrusive technology such as electronic cards or PIN codes.

It's important to understand that the uses of Biometric identification in these cases were not in themselves illegal. It was the process followed by Serco which led to the enforcement action.

Cards and PIN codes have a part to play in the landscape of ID management and verification – although they do have their flaws. They may be shared, lost, forgotten. If an employee's card or PIN is used, you cannot be 100% certain that it was the intended employee who did so.

With Biometric Identification processes, there is an obvious increase in accuracy, security and efficiency of identification. But this must be measured against the increased process you must put in place to manage such a scheme.

THE UPTAKE OF BIOMETRIC IDENTIFICATION TECHNOLOGY, AS OF DECEMBER 2024, VARIES SIGNIFICANTLY BY SECTOR / INSTITUTION...

HEALTHCARE

40%

uptake of biometric identification systems in their T&A workflow

MANUFACTURING & LOGISTICS

30%

uptake

EDUCATION

20%

uptake for attendance tracking – as you might expect, organisations are far more considerate of storing and processing biometric data of children than of adults.

There are many factors that affect the willingness of a workplace to accept the deployment of a Biometric Identification system:

1. GENERATIONAL DIFFERENCES:

- **Gen Z (born roughly 1997-2012):** This generation tends to be more tech-savvy and familiar with biometric technology, such as facial recognition through smartphones and other devices. As a result, they are generally more accepting of biometrics, viewing them as a natural part of technological advancement.
- **Millennials (born roughly 1981-1996):** Similar to Gen Z, Millennials are often quite comfortable with technology and may be more accepting of biometrics, especially if they perceive benefits such as increased convenience and security.
- **Gen X (born roughly 1965-1980):** This group is often more cautious about new technology compared to younger generations. While many are accepting of biometric solutions, they may be more concerned about privacy and data security issues.
- **Baby Boomers (born roughly 1946-1964):** Acceptance among Baby Boomers can vary significantly. While some may embrace the technology for its benefits, others may be more resistant, particularly due to privacy concerns or unfamiliarity with the technology.

2. PRIVACY CONCERNS:

Older generations may express more apprehension regarding the security of biometric data and the potential for misuse. Concerns about data breaches and unauthorised access to personal information can be stronger among older demographics.

3. AWARENESS AND EDUCATION:

Acceptance often correlates with awareness and education about how biometric systems work and how data is protected. Providing clear information and transparency can help alleviate concerns across all age groups.

4. EMPLOYMENT CONTEXT:

The decision to deploy biometric solutions can also depend on the workplace culture and how the technology is introduced. If employees feel involved in the decision-making process and understand the benefits, acceptance rates tend to be higher, regardless of age.

5. CULTURAL FACTORS:

Beyond generational differences, cultural attitudes towards technology, privacy, and security can influence acceptance levels.

There are also a number of factors that UK based companies should consider before embarking on a Biometric based ID solution:

1. REGULATORY COMPLIANCE: Ensure compliance with UK GDPR by obtaining explicit employee consent and implementing proper data handling, storage, and processing practices.

2. DATA SECURITY: Assess the security measures in place to protect biometric data from breaches or unauthorized access. Implement robust encryption methods and secure storage solutions to safeguard employees' biometric information.

3. EMPLOYEE ACCEPTANCE: Gauge employee attitudes towards biometric systems. Conduct surveys or focus groups to understand concerns, preferences, and acceptance levels. Clear communication about the benefits and security measures can enhance acceptance.

4. COST-BENEFIT ANALYSIS: Evaluate the financial implications of acquiring, implementing, and maintaining biometric systems versus potential gains in productivity, accuracy, and security. Consider the long-term ROI.

5. TECHNOLOGY RELIABILITY: Research the accuracy, reliability, and user-friendliness of the biometric technology under consideration. Assess factors such as false acceptance rates, false rejection rates, and ease of use for employees.

6. INTEGRATION WITH EXISTING SYSTEMS: Determine how well the biometric solution will integrate with current human resources or payroll systems. A seamless integration can enhance overall efficiency and reduce operational disruptions.

7.USE CASE SUITABILITY: Evaluate if biometric identification addresses organisational needs like preventing buddy punching, enhancing security, or streamlining attendance tracking.

8. PRIVACY CONCERNS: Address potential privacy issues and ensure that employees feel their biometric information is handled respectfully and securely. Develop clear policies outlining the purpose of data collection and use.

9. TRAINING AND SUPPORT: Plan for employee training and support to ensure smooth implementation and acceptance of the new system. Providing resources and assistance can help ease the transition.

10. CULTURAL CONTEXT: Consider the company culture and how it aligns with the use of biometric technology. Companies with a strong focus on employee privacy and autonomy may face more challenges in adoption.

11. LEGAL AND ETHICAL CONSIDERATIONS: Consult with legal experts to understand any potential legal implications, particularly around discrimination and data protection laws. Ensure ethical considerations are made regarding the deployment of biometric technology.

By carefully weighing these factors, a company can make a more informed decision about whether to incorporate biometric identification into its T&A solution, balancing the potential benefits with the concerns and needs of employees and regulatory requirements.

SUMMARY

Biometric identification offers clear advantages in security, accuracy, and efficiency, but its implementation must be carefully managed to ensure it aligns with regulatory requirements, ethical considerations, and employee expectations. The case of Serco highlights the importance of proportionality and necessity in deploying such technology—organisations must not only comply with legal frameworks but also consider less intrusive alternatives when appropriate.

Successful adoption of biometric systems hinges on striking the right balance between security and privacy. By addressing concerns related to data protection, transparency, and employee consent, businesses can foster greater acceptance of these technologies. Moreover, thoughtful integration with existing systems and clear communication with stakeholders can help mitigate resistance and maximise the benefits.

Ultimately, biometric identification is not a one-size-fits-all solution. Organisations must assess their unique needs, industry norms, and workforce demographics before implementation. When done correctly, biometric authentication can enhance operational efficiency while respecting the rights and privacy of individuals. The key lies in responsible deployment—one that is both technologically sound and ethically grounded.

SYNEL™ | **MAKE** EVERY MINUTE COUNT™

ABOUT SYNEL

Synel UK, part of the Synel MLL PayWay Group, has since 1990 been the preferred choice of countless businesses around the world — investing in a workforce management solution to help them operate more efficiently.

From small factories and warehouses employing just a few people, through to university campuses, healthcare facilities, retail stores and large office complexes — Synel provides customisable, scalable and easy to use systems which help increase productivity and reduce human resource management administration costs.

Synel delivers complete piece of mind by offering unbeatable levels of technical support — with remote and on-site services, backed by an industry-leading extended warranty scheme.

0208 900 9991
sales@syneluk.com

WWW.SYNEL.CO.UK
WORKFORCE MANAGEMENT SOLUTIONS