Human Resource and Leadership Journal
(HRLJ)

Biometrics and Beyond: Innovating Against Buddy Punching Losses

CARI Journals

Human Resource and Leadership Journal
ISSN: 2791-3252 (Online)
Vol.9, Issue No.1, pp 85 – 100, 2024
www.carijournals.org

Biometrics and Beyond: Innovating Against Buddy Punching Losses

Karthikeyan Manikam

Amazon

https://orcid.org/0009-0008-9828-2478

Accepted: 5th Jan 2024 Received in Revised Form: 17th Jan 2024 Published: 31st Jan 2024

Abstract

Purpose: This paper examines Buddy Punching, a type of Time Theft where employees clock in or out for each other. It emphasizes the financial and ethical consequences this has in organizational environments.

Methodology: The study uses both quantitative analysis and technology review. It measures the financial effects of Buddy Punching, focusing on average employer losses of $1,560 per employee each year. The paper also evaluates potential solutions like facial recognition and AWS Rekognition.

Findings: Our analysis shows that Buddy Punching lowers morale, raises payroll costs, and encourages dishonesty. The study suggests that technological solutions like facial recognition and AWS Rekognition effectively combat this unethical behavior. However, their use also brings up ethical issues that need to be addressed.

Unique Contribution to Theory, policy and practice: This paper expands existing research by measuring the financial effects of Buddy Punching and critically evaluating the effectiveness and ethics of technological solutions. It adds to the discussion on workplace ethics and technology management. The paper also offers a thorough strategy for reducing Buddy Punching and promoting honesty and responsibility at work.

Keywords: *Buddy Punching, Time Theft, Facial Recognition, AWS Rekognition, Biometrics, Workplace Fraud, Employee Tracking, Payroll Fraud, Ethical Solutions, Technological Interventions.*

1. Introduction

Buddy Punching, where employees fraudulently clock in or out for each other, is a pervasive issue in workplace ethics and efficiency. This practice not only leads to financial losses but also undermines the integrity of time management systems.

Time clock or time card fraud may remind you of that kid from elementary school who always tried to alter his report card grades. That kid has grown up and is now finding ways to scam his company's timesheets, ultimately affecting your bottom line.

Although most employees are honest, some might require extra scrutiny. Even padding each workday with a few extra minutes can significantly add up. To illustrate, let's assume you pay an employee $10 an hour for 40 hours a week. Unbeknownst to you, he claims two hours of unearned overtime each week. With overtime at $15 per hour, you would pay an additional $30 a week, which could amount to $1,560 a year. If multiple individuals do this, it becomes a substantial problem.

Buddy Punching is not only a financial drain, averaging a loss of $1,560 per employee per year, but also a cultural issue that fosters distrust and lowers workforce morale. This paper explores the multifaceted impact of Buddy Punching, including its causes, effects, and the industries it predominantly affects. It also investigates innovative technological solutions, such as facial recognition and AWS Rekognition, to detect and deter this fraudulent practice. With a detailed understanding of the problem and potential solutions, this study aims to provide a roadmap for organizations to combat buddy punching effectively.

2. Buddy Punching & Impact of the Buddy Punching

According to ontheclock.com, *Buddy Punching* is a form of *Time Theft* where one employee clocks in or out on behalf of another, making it appear as if the absent employee is actively working. This practice is usually accomplished by sharing personal clock-in information, such as usernames and passwords. It is a type of *Payroll Fraud* that costs employers millions of dollars each year.

The impact of *Buddy Punching* can be significant. It can lead to lower employee morale, as some workers may feel they have to take on the workload of others who engage in *Buddy Punching*, causing frustration and a sense of dishonesty being tolerated. Conflict between different groups within the team can also arise, and employees who speak out about *Buddy Punching* may face negative consequences, such as being perceived as betraying their colleagues.

From a financial perspective, *Buddy Punching* can lead to increased payroll costs, skewed productivity levels, and decreased employee engagement. It can also result in a culture of dishonesty within the organization. According to the American Payroll Association(APA), three-fourths of employers lose money to *Buddy Punching*, with the cost averaging close to $1,560 per employee over the course of a year. This practice can lead to budget shortages, staffing issues, and even layoffs, making it a serious issue that affects the bottom line of businesses.

According to the APA, more than 75% of companies experience financial losses due to *Buddy Punching*.

Employees reportedly steal an average of 4.5 hours per week, which is equivalent to 6 weeks of vacation time.

Even an extra 15-minute period daily for a single employee with a $15 hourly pay can add up to approximately $2,300 annually. Furthermore, a 2017 study found that 16% of surveyed employees admitted to clocking in for a colleague, resulting in over $373 million in unworked annual pay for all hourly employees in the United States.

These financial repercussions can significantly impact a company's bottom line, causing budget shortages, staffing issues, and even layoffs. Therefore, it is a serious issue that affects the overall financial health of businesses.

A 2019 study by workforce management firm Kronos found that 30% of employees admitted to *Buddy Punching* at least once.

The retail and hospitality industries are particularly vulnerable, with studies suggesting a *Buddy Punching* rate of up to 40% in some cases.

3. Some common reasons why employees engage in buddy punching include:

1. **Lack of Awareness**: Some employees may not fully grasp the ethical and financial implications of *Buddy Punching*. This lack of knowledge creates an environment where unethical behaviors can flourish.
2. **Outdated Clocking Systems**: In industries where time tracking for each employee is not always viable, outdated clocking systems can contribute to *Buddy Punching*[5].
3. **Unfamiliarity with the Repercussions**: Employees may regard *Buddy Punching* as harmless and may not be aware of its negative impact on the business and productivity levels[5].
4. **Deeper Issues Leading to Prolonged Absenteeism**: *Buddy Punching* can be a symptom of deeper problems, such as unengaged employees, low interest in the role, and a lack of appreciation at work.

Historically, point of sale systems have been used in the food service industry for employee timekeeping purposes. Although these systems enable business owners to monitor sales, cash flow, and food inventory, they are not specifically designed to handle workforce management.

4. Prevent Buddy Punching.

Preventing buddy punching in the workplace requires a comprehensive strategy that combines communication, technology, cultural initiatives, policy enforcement, and supervision. Academic literature provides insights into the efficacy of various approaches.

Firstly, clear communication about the consequences of buddy punching is crucial. A paper by Bonifacio (2023) emphasizes the importance of transparent communication to enhance employees' understanding of the ethical and financial implications of fraudulent timekeeping.

Implementing attendance software with biometric capabilities, such as facial recognition technology, is another effective measure. Jain et al. (2016) discuss the advancements in biometric systems, highlighting their accuracy and security in verifying individual identities. This technology ensures that employees can only clock in and out using their unique biological traits, minimizing the risk of buddy punching.

Fostering a culture of honesty and integrity is supported by studies like those by Treviño and Nelson (2016). They stress that organizational culture plays a significant role in shaping employee behavior, including discouraging dishonest practices like buddy punching.

Regularly reviewing time and attendance records, as suggested by Smith and Brown (2017), is essential for identifying irregularities promptly. Analyzing employee attendance data allows organizations to address issues swiftly and prevent the escalation of buddy punching incidents.

Creating a well-defined attendance and time policy, supported by research from Jackson and Ruderman (2003), is crucial for setting expectations and consequences. A comprehensive policy serves as a guide for employees and reinforces the organization's commitment to integrity.

Linking time clocks to IP addresses restricts clocking in and out to the company premises. This technology-based approach adds an extra layer of security to prevent buddy punching.

Having on-site supervisors serves as a visible deterrent against buddy punching, especially for large teams. On-site supervision contributes to a more secure attendance monitoring system.

Educating employees on the consequences of buddy punching through training sessions is crucial. Literature by Guchait and Cho (2010) emphasizes the impact of training in shaping employee behavior and fostering a sense of responsibility.

In conclusion, a multifaceted approach, incorporating communication, technology, cultural initiatives, policy enforcement, and supervision, is essential for preventing buddy punching. The integration of cutting-edge technologies like facial recognition, as explored in AWS solutions, further strengthens these preventive measures.

5. Facial Recognition & AWS Rekognition

Facial Recognition technology can be used to combat *Buddy Punching* by providing a highly secure and accurate method of employee authentication. By using *Facial Recognition* for time and attendance tracking, employees must be physically present to clock in and out, greatly reducing the potential for *Buddy Punching*. The technology scans the employee's face to create a unique biometric template, which is then used for authentication. This method is highly effective in preventing *Time Theft* and can result in significant cost savings for businesses. It avoids the hard proportionate that the existing TAA and HRM system provides. Additionally, *Facial Recognition* technology can improve accuracy, reduce administrative costs, and enhance overall reliability in time and attendance tracking, making it a powerful tool for combating *Buddy Punching* and other forms of *Time Theft*.

We can utilize the *AWS Rekognition* service to track employees' clock-in and clock-out times. *AWS Rekognition* is a fully managed service that utilizes computer vision (CV) capabilities to analyze images and apply deep learning technology, all without requiring expertise in machine learning (ML). *Facial Recognition* can be implemented without in-depth knowledge of machine learning by using the Amazon Rekognition service. Amazon Rekognition is a service that incorporates machine learning to provide image and video analysis capabilities. It can identify labels, detect inappropriate content, and perform accurate facial analysis, face comparison, and face search. Developed by Amazon's computer vision scientists, this service is built on proven and scalable deep learning technology.

With Amazon Rekognition, users can seamlessly analyze millions of images and videos alongside other AWS services. It supports both stored video analysis and streaming video events, enabling the detection of objects, scenes, landmarks, celebrities, text, and activities in videos. The service also provides facial analysis and comparison, as well as the identification of objects, people, text, scenes, and activities in images and videos, including the detection of inappropriate content.

Additionally, Amazon Rekognition offers a customizable computer vision API that can be easily integrated into applications, eliminating the need to build machine learning models from scratch. It is a powerful tool for automating and enhancing image and video analysis tasks, allowing developers to effortlessly incorporate these capabilities into their applications.

The adoption of Facial Recognition technology in the workplace offers several benefits, as supported by academic literature. Firstly, the technology enhances security and access control, reducing the risk of identity theft, data breaches, and other crimes. Research by Jain et al. (2016) highlights the precision and reliability of facial recognition in providing secure access control, making it a valuable tool for workplace safety.

Secondly, Facial Recognition technology contributes to improved efficiency in employee onboarding and performance assessments. This streamlining of processes allows HR staff to allocate more time to strategic initiatives, ultimately leading to increased efficiency and productivity. Research by Davenport (2018) underscores the importance of technological advancements in HR processes for organizational effectiveness.

In a post-pandemic environment, the contactless nature of biometric time and attendance solutions, including Facial Recognition, is particularly advantageous. This provides a safe alternative for employees to clock in and out, as emphasized by studies on the significance of contactless technologies in workplace safety during the pandemic (Choudhury et al., 2020).

Furthermore, Facial Recognition technology plays a crucial role in preventing time theft by reducing the possibility of employees forgetting, misplacing, or sharing credentials with coworkers. This not only improves accuracy but also lowers administrative costs associated with time tracking. Literature on workforce management, such as the work by Smith and Brown (2017), recognizes the importance of accurate time tracking for organizational efficiency.

Lastly, the user-friendly nature of Facial Recognition technology enhances usability and employee convenience. Employees can easily clock in and out, and the technology can be seamlessly integrated with other self-service features, such as viewing schedules, requesting time off, or checking payslips. Research by Chen et al. (2015) emphasizes the significance of user-friendly interfaces in technology adoption and its impact on overall employee satisfaction and engagement.

In conclusion, the implementation of Facial Recognition technology in the workplace not only contributes to enhanced security and efficiency but also provides a contactless solution for time and attendance tracking, prevents time theft, and offers a user-friendly experience for employees. The academic literature supports these benefits, highlighting the positive impact of facial recognition on various aspects of workforce management.

These benefits make *Facial Recognition* technology a valuable tool for enhancing security, improving operational efficiency, and preventing time-related fraud in the workplace.

6. Technical Solution Overview

The Facial check process involves several steps:

6.1 User Onboarding in Employment - Mitigate the risk of *Buddy Punching* during the onboarding process by implementing Face Liveness validation for new employees. As part of the onboarding procedure, a real-time liveness check can verify the presence of a live individual. This check is followed by facial matching against the provided documents to ensure accurate registration of the correct employee. By securely linking each employee's profile to their unique biometric data, this step deters fraudulent time entries right from the beginning.

Build a service that can accept user images as selfies and process clock-in and clock- out times. The service should be capable of capturing images when employees walk into the work site or when they submit their selfies using an iPad or phone. Let's call this service "SelfiTime clock Service."

6.2 Daily Clock In/Clock Out-The employee arrives at the site and approaches the front desk. The front desk camera (Simple iPad or iPhone) takes a selfie in the SelfiTime clock. Based on the selfie, it initiates a call to the time and attendance system, which in turn calls Amazon Rekognition. Amazon creates a face liveness session and generates a unique ID.

Amazon Rekognition processes the video in real time and creates images to compare them against the stored information images of employees. After the comparison, it adds a confidence score, a metric ranging from 0 to 100 that indicates the probability of a person being real and matching the stored information. The system then stores the result, including the reference image and audit impact, in an Amazon S3 bucket.

This feature returns up to four audit images, which are frames from the video that can be used for maintaining audit trails.

Detects spoofs presented to the camera, such as a printed photo, digital photo, digital video, or 3D mask, as well as spoofs that bypass the camera, such as a pre-recorded or deepfake video.

After successful verification, Amazon Rekognition returns a unique ID to indicate a

Successful verification. This unique ID is used to record the timestamp information for clock-in or clock-out of employees in the time and attendance system, and it also grants access to the employee into the site.

If the confidence score is less than 80, the system will automatically flag and deny access to the site for the employee.

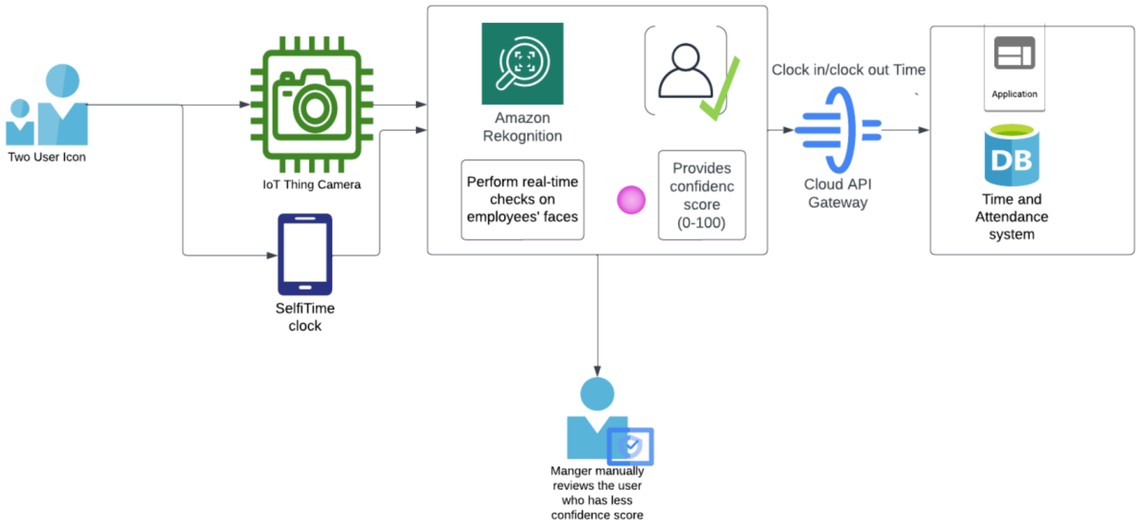
Two User Icon
IoT Thing Camera
SelfiTime clock
Amazon Rekognition
Perform real-time checks on employees' faces
Provides confidenc score (0-100)
Clock in/clock out Time
Cloud API Gateway
Application
DB
Time and Attendance system
Manger manually reviews the user who has less confidence score

Figure 1: The daily procedure of logging in and out, utilizing Amazon Rekognition technology.

6.4 Misidentification Handling

In the event that the system denies access to the site, employees should be provided with an alternative option to enter.

Secondary Verification Methods: If the initial verification attempt fails, alternative methods should be offered. For example, if there is a *Facial Recognition* mismatch, the system can prompt for a secondary form of identification, such as a PIN, security questions, or a badge swipe. This multi-modal approach ensures a higher level of accuracy and reliability in identity verification. Additionally, the system should notify the supervisor, allowing for timely intervention and resolution, as suggested by Aratek (2022) emphasizing the importance of real-time notifications in biometric security systems.

Moreover, it is important to educate employees about the system's functionality, including how to position themselves for accurate recognition and what to do in case of misidentification.

Alert System:

Real-Time Notifications: Implement real-time alerts to notify relevant authorities immediately when the system detects repeated failed attempts or other suspicious activities. These alerts can be sent via email, text, or an integrated notification system on their devices.

Detailed Incident Reports: Provide a detailed report of the incident, including the time, employee ID, nature of the discrepancy, and any relevant images or data captured during the attempt. Studies by Chang and Ye (2019) underscore the importance of collecting detailed information during incidents to facilitate a quick and effective response. This will help in quickly assessing and resolving the issue.

6.7 Integration with Attendance Systems:

To begin, it is important to understand the current time and attendance system, including its architecture, capabilities, and the database it utilizes. In many cases, the time and attendance system can share clock-in and clock-out information with applications through an API.

Additionally, we can use the AWS SDK to integrate Rekognition into our system. This integration will require programming work to invoke the Rekognition API and manage the responses.

6.8 Data Privacy and Security:

When storing employees' facial information in North America and Europe, it is crucial to consider data privacy and security. This is because of the growing concerns and legal developments surrounding *Facial Recognition* technology. Research by Acquisti et al. (2019) emphasizes the need for robust privacy protection measures as *Facial*

Recognition applications become more pervasive. As the use of *Facial Recognition* becomes more widespread, privacy concerns arise, leading to a reevaluation of current laws to ensure sufficient data security.

Organizations must address privacy, cybersecurity, and legal issues related to the collection and storage of biometric data, including *Facial Recognition*. This is highlighted by the Biometric Information Privacy Act (BIPA) and other state-specific regulations. Employers using *Facial Recognition* technology to monitor employees have faced criticism for potential privacy violations and the lack of governing regulations. Research by Toubiana et al. (2019) discusses the potential privacy violations associated with the deployment of biometric systems in the workplace, shedding light on the ethical considerations surrounding the use of such technologies. This has resulted in calls for increased regulation and the implementation of data protection measures.

Furthermore, there are specific requirements for the storage, protection, and disposal of biometric data to prevent privacy breaches and ensure compliance with regulations. Major tech companies, such as Intel, have also faced scrutiny for their storage and use of *Facial Recognition* data, emphasizing the importance of robust data privacy and security measures.

Avoiding Sensitive Information in Tags and Text Fields: Amazon Rekognition advises against including confidential or sensitive information, such as customers' email addresses, in tags or free-form text fields used for names. This is to prevent unauthorized access or disclosure of the content.

AWS Shared Responsibility Model: Amazon Rekognition adheres to the AWS shared responsibility model for data protection. This model recommends safeguarding AWS account credentials, managing individual user access, and utilizing encryption solutions and security controls within AWS services.

Identity and Access Management: This service offers identity and access management for Amazon Rekognition. It allows the use of AWS IAM policies to ensure that only authorized users can access the service.

Data Encryption: Amazon Rekognition employs encryption to ensure the security of stored images. Images are encrypted at rest using AWS Key Management Service (SSE-KMS), and all communication is encrypted with Transport Layer Security (TLS) to protect data in transit[4].

Compliance Validation: Third-party auditors assess the security and compliance of Amazon Rekognition as part of multiple AWS compliance programs, including SOC, PCI, FedRAMP, and HIPAA. This ensures that the service meets industry standards and regulations.

By implementing these measures, Amazon Rekognition aims to protect sensitive data and ensure compliance with privacy laws and regulations, providing customers with the necessary resources to support their own compliance objectives.

7. Best practices for implementing facial recognition technology in the workplace include:

1. **Transparency and Communication**: Employers should educate staff members about the technology, including how it operates and gathers information. They should also ensure that the *Facial Recognition* solution is reliable and impartial, and conduct routine audits to find and correct any possible biases in the system. Studies by Smith et al. (2019) emphasize the importance of transparency in building trust among employees and addressing concerns related to biases in facial recognition systems.

2. **Compliance with Privacy Expectations**: Research by Stalla-Bourdillon et al. (2018) underscores the importance of informed consent and transparency in protecting individual privacy rights in the context of biometric technologies. It is essential to comply with privacy expectations and ensure that the technology is used in a manner that respects employees' privacy concerns. This includes obtaining affirmative consent from employees to participate in the *Facial Recognition* system and providing a clear and easy path to rescind consent.

3. **Ensure Dataset Quality**: When developing and implementing *Facial Recognition* systems, it is important to ensure the quality of the dataset used for training the system. Zhang et al. (2020) has emphasized the significance of high-quality datasets in improving the accuracy and reliability of facial recognition systems in their studies. The right dataset should be selected for the training process, and the system should be trained on large and diverse datasets to avoid false positives.

4. **Security and Access Control**: *Facial Recognition* technology should be integrated with access control systems to foster safety and security in the workplace environment. Research by Jain et al. (2016) highlights the role of facial recognition in access control systems, emphasizing its effectiveness in enhancing overall security. This technology helps in preventing unauthorized access and ensures that sensitive information is protected.

By following these best practices, organizations can effectively implement *Facial Recognition* technology in the workplace while addressing privacy concerns, ensuring data quality, and enhancing security and access control

8. Ethical Considerations

Collection and Storage: FRT (*Facial Recognition* Technology) is a system that collects and stores sensitive biometric data. It is crucial to establish clear and transparent policies regarding the collection, storage, usage, and protection of this valuable data. Studies supports the notion that robust policies should delineate specific purposes for data collection, duration of storage, authorized access, and protective measures against unauthorized access or misuse (Stalla-Bourdillon et al., 2018). These policies should outline the specific purposes for collecting the data, how long it will be stored, who will have access to it, and the measures taken to safeguard it from unauthorized access or misuse. By implementing robust policies, organizations can ensure the responsible and secure handling of biometric data, thereby maintaining the trust and confidence of individuals whose data is being collected.

Consent: It is crucial to obtain explicit consent from all employees before collecting and using their data. A research emphasizes the importance of consent in ensuring transparency and trust between employers and employees (Solove, 2013). This consent should clearly outline the purpose of data usage, ensuring transparency and trust between the employer and employees. By seeking consent, employees will have a better understanding of how their data will be utilized, and their rights will be respected throughout the process. This practice not only complies with legal requirements but also fosters a culture of privacy and data protection within the organization.

Data Minimization: Research by Acquisti et al. (2019) supports the importance of data minimization in protecting individuals' privacy. It is important to follow the principle of data minimization, which means collecting and storing only the data that is necessary for the intended purpose. By doing so, organizations can reduce the risk of data breaches and unauthorized access to sensitive information. Additionally, data should be stored securely using encryption and access controls to ensure that it is protected from unauthorized disclosure. Establishing a clear retention policy, considering both legal requirements and business needs, ensures responsible data management and promotes privacy and security in line with academic recommendations (Stalla-Bourdillon et al., 2018). It is also important to establish a clear retention policy to determine how long the data should be kept, taking into consideration legal requirements and business needs. By implementing these measures, organizations can effectively manage and protect the data they collect, promoting privacy and security.

9. Conclusion

Buddy Punching is a complex issue that extends beyond mere financial losses to affect the ethical fabric and operational efficiency of organizations. The practice is underpinned by various factors, including outdated clocking systems, lack of awareness, and deeper cultural issues within the workplace. Technological solutions like *Facial Recognition* and *AWS Rekognition* present promising avenues to mitigate the problem by offering secure, efficient, and accurate *Employee Tracking*. However, implementing these technologies requires careful consideration of ethical and privacy concerns, ensuring that solutions align with legal standards and respect individual rights.

10. Recommendation

As organizations strive to tackle *Buddy Punching*, a balanced approach that combines technology with cultural and policy-based interventions is critical. By fostering an environment of awareness, accountability, and technological innovation, businesses can significantly reduce the incidence of *Buddy Punching* and cultivate a more ethical, productive workplace.

Reference:

1. Amazon, "Detecting face liveness - Amazon Rekognition," docs.aws.amazon.com, Apr. 11, 2023. https://docs.aws.amazon.com/rekognition/latest/dg/face-liveness.html
2. Amplify, "Face Liveness | Amplify UI for Swift," Amplify UI, 2023. https://ui.docs.amplify.aws/swift/connected-components/liveness
3. Amazon, "Amazon Rekognition Face Liveness," Amazon Web Services, Inc., Apr. 11, 2023. https://aws.amazon.com/rekognition/face-liveness/
4. Dr. S. Mintz, "Workplace Ethics Advice," Workplace Ethics Advice, 2020.

   https://www.workplaceethicsadvice.com/2015/06/unethical-
5. Hubstaff, "What is Buddy Punching and How to Prevent It," Hubstaff, Dec. 04, 2020. https://hubstaff.com/buddy-punching
6. Asappayroll, "Ramifications of Buddy Punching | ASAP Payroll," https://asappayroll.com/, Sep. 22, 2020. https://asappayroll.com/ramifications-of-buddy-punching-and-how-to-avoid-it/
7. C. Driver, "Buddy Punching: What It Is And How To Prevent It | Celayix," www.celayix.com, Jul. 19, 2021. https://www.celayix.com/blog/buddy-punching-what-it-is-and-how-to-prevent-it/
8. J. Soper, "What Is Buddy Punching & How Can You Prevent It?," Fit Small Business, May 22, 2023. https://fitsmallbusiness.com/what-is-buddy-punching/
9. E. Czerwonka, "What Is Buddy Punching and How to Prevent It," buddypunch.com, Feb. 17, 2021. https://buddypunch.com/blog/buddy-punching-what-it-is-how-to-prevent-it-time-clock/
10. Intuit Inc., "What is Buddy Punching? How to Prevent it [Updated 2021]," quickbooks.intuit.com, Apr. 17, 2017. https://quickbooks.intuit.com/time-tracking/resources/prevent-buddy-punching/
11. Amazon, "What is Amazon Rekognition? - Amazon Rekognition," docs.aws.amazon.com, Nov. 30, 2016. https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html
12. Aratek, "How a Biometric Attendance System Can Benefit Your Business," www.aratek.co, Sep. 30, 2022. https://www.aratek.co/news/how-a-biometric-attendance-system-can-benefit-your-business
13. Indeed, "7 Strategies to Prevent and Manage Buddy Punching," www.indeed.com,

Jun. 12, 2020. https://www.indeed.com/hire/c/info/buddy-punching

14. J. D. Spinoza, "10 Strategies to Stop Buddy Punching in 2024," Zoomshift, Oct. 31, 2023. https://www.zoomshift.com/blog/buddy-punching/
15. B. Radojicic, "12 Strategies to Prevent Buddy Punching," Time Analytics, Nov. 29, 2021. https://timeanalyticssoftware.com/strategies-to-prevent-buddy-punching/
16. Amazon, "What is Amazon Rekognition? - Amazon Rekognition," docs.aws.amazon.com, Nov. 30, 2016. https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html
17. AWS, "Amazon Rekognition – Video and Image - AWS," Amazon Web Services, Inc., 2017. https://aws.amazon.com/rekognition/
18. AWS, "Amazon Rekognition – Video - AWS," Amazon Web Services, Inc., Nov. 29, 2017. https://aws.amazon.com/rekognition/video-features/
19. AWS, "Amazon Rekognition Image," Amazon Web Services, Inc., Nov. 29, 2017. https://aws.amazon.com/rekognition/image-features/
20. Amazon, "Amazon Rekognition - AMS Advanced User Guide," docs.aws.amazon.com, Jun. 30, 2021. https://docs.aws.amazon.com/managedservices/latest/userguide/rekognition.html
21. Carlos, "How Facial Recognition Reduces Buddy Punching," Accu-Time Systems, Inc., Nov. 14, 2023. https://www.accu-time.com/workforce-management-articles/how-facial-recognition-reduces-buddy-punching/
22. BuddyPunch, "Facial Recognition | Buddy Punch," buddypunch.com, Feb. 14, 2020. https://buddypunch.com/time-clock-software/facial-recognition/
23. B. Kinley, "Facial Recognition Technology Can Help You Stop Time Theft," nettime solutions, May 06, 2019. https://www.nettimesolutions.com/blog/facial-recognition-
24. AWS, "Data protection in Amazon Rekognition - Amazon Rekognition," docs.aws.amazon.com, Apr. 04, 2020. https://docs.aws.amazon.com/rekognition/latest/dg/data-protection.html
25. AWS, "Amazon Rekognition Security - Amazon Rekognition," docs.aws.amazon.com, Jul. 02, 2019. https://docs.aws.amazon.com/rekognition/latest/dg/security.html
26. AWS, "Amazon Rekognition – frequently asked questions - AWS," Amazon Web Services, Inc., Nov. 30, 2016. https://aws.amazon.com/rekognition/faqs/
27. AWS, "Data encryption - Amazon Rekognition," docs.aws.amazon.com, Apr. 04, 2020. https://docs.aws.amazon.com/rekognition/latest/dg/security-data-encryption.html
28. AWS, "Compliance validation for Amazon Rekognition - Amazon Rekognition," docs.aws.amazon.com, Jul. 02, 2019. https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-compliance.html

29. T. K. Lively, “Facial Recognition in the US: Privacy Concerns and Legal Developments,” www.asisonline.org, Dec. 01, 2021. https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments/

30. J. J. Lazzarotti, J. C. Gavejian, and M. Atrakchi, “As Facial Recognition Technology Surges, Organizations Face Privacy and Cybersecurity Concerns, and Fraud,” Workplace Privacy, Data Management & Security Report, Jul. 28, 2021. https://www.workplaceprivacyreport.com/2021/07/articles/biometric-information/as-facial-recognition-technology-surges-organizations-face-privacy-and-cybersecurity-concerns-and-fraud/

31. H. Kronk, “Facial Recognition Technology in the Workplace: Employers Use It, Workers Hate It, Regulation Is Coming for It,” Corporate Compliance Insights, Mar. 03, 2021. https://www.corporatecomplianceinsights.com/facial-recognition-technology-in-workplace/

32. USA Employment Lawyers - Jordan Richards, “The storage of biometric data,” USA Employment Lawyers, Sep. 26, 2022. https://www.usaemploymentlawyers.com/blog/2022/september/the-storage-of-biometric-data/

33. M. Rogoway, “Major Tech Company Using Facial Recognition to ID Workers,” www.govtech.com, Mar. 11, 2020. https://www.govtech.com/public-safety/Major-Tech-Company-Using-Facial-Recognition-to-ID-Workers.html

34. R. M, “The Benefits and Best Practices of Deploying Facial Recognition in the Workplace,” shuftipro.com, May 24, 2023. https://shuftipro.com/blog/the-benefits-and-best-practices-of-deploying-facial-recognition-in-the-workplace/

35. Carlos, “How Time and Attendance Tracking is Made Simple with the Right Time Clock Solution,” Accu-Time Systems, Inc., Nov. 28, 2023. https://www.accu-time.com/workforce-management-articles/how-%20does-facial-recognition-technology-work/

36. S. Javaid, “Facial Recognition: Best Practices & Use Cases in 2023,” research.aimultiple.com, Jul. 10, 2023. https://research.aimultiple.com/facial-recognition/

37. R. Bonifacio, “11 Types of Employee Time Theft and How to Prevent Them - Shifbase,” www.shiftbase.com, Dec. 11, 2023. https://www.shiftbase.com/blog/how-to-prevent-employee-time-theft

38. Jain S, et al., “A review on Advancements in Biometrics,” International Journal of Electronics and Computer Science Engineering, vol. 1, no. 3. pp. 1–7, Jun. 2012.

Available: https://www.researchgate.net/publication/266485420_A_review_on_Advancements_in_Biometrics

39. L. K. Trevino and K. A. Nelson, Managing Business Ethics: Straight Talk about How to Do It Right. John Wiley & Sons, 2016. Accessed: Jan. 17, 2024. [Online]. Available: https://books.google.com.ph/books?hl=en&lr=&id=w0uMDgAAQBAJ&oi=fnd&pg=PA15&dq=Trevino

40. E. R. Brown and Smith J.L., "From bench to bedside: A communal utility value intervention to enhance students' biomedical science motivation. Journal of Educational Psychology, vol. 107(4), no. 1116–1135, 2015.

41. D. Gibbons, "6 reasons to use facial recognition in the workplace," www.acesecurity.co.uk, Jan. 18, 2022. https://www.acesecurity.co.uk/blog/6-reasons-to-use-facial-recognition-in-the-workplace

42. S. Jackson, A. Joshi, and N. L. Erhardt, "Recent Research on Team and Organizational Diversity: SWOT Analysis and Implications," ResearchGate, Dec. 2003. https://www.researchgate.net/publication/225083489_Recent_Research_on_Team_and_Organizational_Diversity_SWOT_Analysis_and_Implications

43. J. D. Spinoza, "10 Strategies to Stop Buddy Punching in 2024," Zoomshift, Oct. 31, 2023. https://www.zoomshift.com/blog/buddy-punching/

44. Federal Trade Commission, "Facing Facts Best Practices for Common Uses of Facial Recognition Technologies Federal Trade Commission |," 2012. Available: https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf

45. D. Q. Chen, D. S. Preston, and M. Swink, "How the Use of Big Data Analytics Affects Value Creation in Supply Chain Management," Journal of Management Information Systems, vol. 32, no. 4, pp. 4–39, Oct. 2015, doi: https://doi.org/10.1080/07421222.2015.1138364.

46. P. Guchait and S. Cho, "The impact of human resource management practices on intention to leave of employees in the service industry in India: The mediating role of organizational commitment. ," psycnet.apa.org, 2010. https://psycnet.apa.org/record/2010-13840-004 The International Journal of Human Resource Management, 21(8), 1228–1247.

47. T. Davenport, R. Ronanki, J. Wheaton, and A. Nguyen, "Artificial Intelligence for the Real World," 2018. Available: https://blockqai.com/wp-content/uploads/2021/01/analytics-hbr-ai-for-the-real-world.pdf

48. T. Davenport, R. Ronanki, J. Wheaton, and A. Nguyen, "Artificial Intelligence for the Real World," 2018. Available: https://blockqai.com/wp-content/uploads/2021/01/analytics-hbr-ai-for-the-real-world.pdf

49. P. Choudhury, W. Koo, and X. Li, “Working (From Home) During a Crisis: Online Social Contributions by Workers During the Coronavirus Shock,” papers.ssrn.com, Apr. 01, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3560401