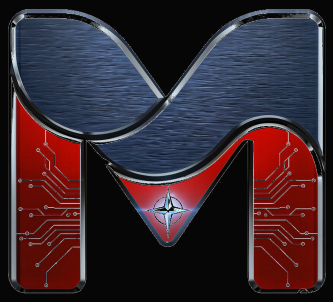

MICKAI EBOOK SERIES · PLAYBOOK No. 4

AI in the Workplace. From Opaque Surveillance to Cryptographic Accountability.

A response to Professor Nazrul Islam's Guardian column on 11 May 2026, and an engineering playbook for the worker, the union, the employer, and the regulator at the same chain.

AUTHOR

Micky Irons

Founder and named inventor, Mickai LTD.

EBOOK · No. 4 IN A SERIES OF 14

Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk

UK IPO patent family GB2607309.8 to GB2610422.4 · Trade mark UK00004373277

Crunchbase · LinkedIn · GitHub · mickai.co.uk

DATE · 14 May 2026 · v1

EBOOK · No. 4 IN A SERIES OF 14

Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk

TABLE OF CONTENTS

Contents

Foreword

A note from the author

Part I · The Guardian Framing

1. The Guardian column, in summary
2. The two-tier workforce divide
3. The wider 2026 record

Part II · The Engineering Question Underneath

4. Vendor-key, vendor-format, vendor-cloud
5. The cryptographic position the worker should hold
6. The cryptographic position the union should hold

Part III · The Substrate Answer

7. Trust-domain externalisation in plain terms
8. The same chain for four parties at once
9. The browser-resident verifier in the worker's hand

Part IV · Policy Fit

10. UK GDPR Article 22 in practice
11. ICO workplace monitoring guidance
12. Engagement path with the TUC and the academy

Appendix

About the author
References and further reading

FOREWORD

A note from the author

Professor Nazrul Islam used his Guardian column on 11 May 2026 to name AI's real workplace threat: opaque AI-powered systems of surveillance and control of lower-autonomy workers. The framing is editorial. The engineering framing underneath it is that the opacity is structural.

This ebook reads the Guardian framing, walks the engineering question underneath, and proposes the cryptographic accountability answer. The same chain that satisfies the operator's audit obligation also satisfies the worker's Article 22 challenge, the union's grievance procedure, and the ICO's incident review.

The Mickai substrate primitives are filed at the UK Intellectual Property Office across the GB2607309.8 to GB2610422.4 patent family. The trade mark Mickai is registered at UK00004373277.

Micky Irons

Founder and named inventor, Mickai LTD · 14 May 2026

PART I · THE GUARDIAN FRAMING

What Nazrul Islam actually argued

1. The Guardian column, in summary

Professor Nazrul Islam's column reads the 2026 workplace through a two-tier lens. Higher-autonomy workers use AI as a productivity instrument and accumulate the gains. Lower-autonomy workers are surveilled by AI for productivity, behaviour, and compliance, and absorb the costs. The asymmetry, Islam argues, is the policy question that needs answering.

The editorial framing names the asymmetry. The engineering framing underneath it asks what cryptographic position would close the gap. The rest of this ebook is the answer to that question.

2. The two-tier workforce divide

Across the UK economy in 2026, the divide between AI-as-tool and AI-as-overseer is sharper than at any point since the introduction of digital time-and-motion systems in the early 2000s. A senior manager at a UK plc uses ChatGPT, Claude, and Copilot to draft, summarise, and analyse; the same employer deploys workforce management AI on shift-based and customer-facing roles to score, monitor, and route the lower-autonomy workforce.

The 2026 record (CNBC, The Register, The Week, the TUC's annual digital workforce report) documents the asymmetry. The substrate question is whether the lower-autonomy worker can hold an evidentiary position against the system that surveils them.

3. The wider 2026 record

Beyond Islam's column, the wider record in May 2026 documents the same pattern across CNBC, The Register, and The Week. The pattern is consistent: AI surveils the lower-autonomy workforce in vendor-key, vendor-format, vendor-cloud configurations; the worker has no cryptographic position against the surveillance; the employer has no replayable audit trail; the regulator (ICO, ACAS, the relevant Employment Tribunal) has no chain of custody.

PART II · THE ENGINEERING QUESTION UNDERNEATH

What the structural opacity actually is

4. Vendor-key, vendor-format, vendor-cloud

Workplace AI surveillance products (the major workforce management platforms, the call-centre AI scoring vendors, the warehouse productivity systems, the gig-economy dispatch AIs) hold the audit trail in the vendor's database under the vendor's key in the vendor's format. The employer is the customer; the worker is the data subject; the regulator is the third party. None of them controls the cryptographic position.

The opacity is not a product defect. It is the deployment model.

> **Vendor-key audit is the structural opacity Islam's column names.**

5. The cryptographic position the worker should hold

The worker should hold a public key. Every AI action that affects the worker (scoring, scheduling, ranking, monitoring, classification) should produce a record signed under the operator's hardware key. The worker should be able to replay the chain on their phone, six months after the fact, and arrive at a deterministic verdict per action that affected them.

That position is independent of the worker's employer continuing to exist, the AI vendor continuing to exist, or the worker continuing to be employed. The chain verifies under the operator's key regardless of downstream events.

6. The cryptographic position the union should hold

The union representative needs the same position. When the worker raises a grievance, the union's first step is reconstruction. With a vendor-shaped audit log, reconstruction is a request to the employer's people-systems team and a long wait. With an OAR chain, reconstruction is a verifier run on the union's own laptop with the worker's chain file.

The union's role moves from advocacy under uncertainty to advocacy on cryptographic evidence. The grievance procedure changes character.

PART III · THE SUBSTRATE ANSWER

Trust-domain externalisation for the workplace

7. Trust-domain externalisation in plain terms

Trust-domain externalisation is the architectural pattern where the audit trail of an AI decision is held under the operator's key in an open format, replayable by any party the operator authorises with the chain and the public key. Applied to the workplace surveillance surface, the pattern reads: the employer holds the chain, the worker holds the public key, the union holds the verifier, the ICO walks the chain on incident review.

The pattern works because each party holds a different artefact, but all four artefacts together produce a deterministic verdict. No single party can suppress the verdict by withholding their artefact.

8. The same chain for four parties at once

The structural property the substrate produces is that four different parties walk the same chain and arrive at the same verdict. The worker, the union representative, the employer's HR function, and the ICO investigator all run the verifier on the same chain file with the same public key. The output is the same record-by-record verdict array.

The structural property policy alone cannot produce is precisely this property. Policy assigns roles; the substrate produces deterministic outputs across the roles.

9. The browser-resident verifier in the worker's hand

The verifier ships as a static web page that runs offline in any browser. The worker scans a QR code on a payslip or a shift-management screen, the QR code carries the chain file URI and the public key hash, the verifier loads, the worker sees the verdict for every AI action that affected them across the chain.

The user-experience point is that no app installation is required. The verifier is a URL. The worker's cryptographic position is, in practice, a bookmark.

PART IV · POLICY FIT

UK GDPR Article 22, ICO guidance, TUC engagement

10. UK GDPR Article 22 in practice

UK GDPR Article 22 gives the data subject the right not to be subject to a decision based solely on automated processing that produces legal effects or similarly significantly affects them. The right exists; exercising it requires evidence. The OAR chain is the evidence the data subject's representative walks into the Article 22 challenge with.

Without the chain, the Article 22 challenge is a procedural matter. With the chain, the Article 22 challenge is a cryptographic matter; the verifier output is the artefact at tribunal.

11. ICO workplace monitoring guidance

The ICO's workplace monitoring guidance, refreshed across 2024 and 2025, sets the data protection floor for workplace surveillance. The guidance is policy-oriented and assumes the employer will provide evidence on request. The OAR chain operationalises 'on request' as a chain file plus a public key; the ICO's investigator runs the verifier and produces the same verdict the worker's representative produces.

12. Engagement path with the TUC and the academy

The Trades Union Congress is the natural counterparty for the substrate engagement. The TUC's digital workforce policy team can receive a thirty-minute substrate briefing under the existing engagement framework. The academic counterparty (Professor Islam's research base, the Centre for Industrial Relations at Warwick, the wider AI-and-labour research community) can read the chain primitives against the policy argument.

Engineering leadership at major UK employers, union representatives, ICO digital-policy desk, and the academic AI-and-labour community is open to a fifteen-minute substrate briefing at any time. press@mickai.co.uk.

APPENDIX · ABOUT THE AUTHOR

Micky Irons

Founder of Mickai LTD (Companies House 17166618, England and Wales, registered office 20 Wenlock Road, London, N1 7GU). Named inventor on the Mickai SIOS patent corpus, recorded on the UK Intellectual Property Office public register at numbers GB2607309.8 to GB2610422.4. Trade mark Mickai registered at UK00004373277 (classes 9 and 42, filed 15 April 2026).

Before founding Mickai, Micky was a Sellafield site worker. The egress constraint observed from inside the regulated workstation is the engineering origin of the substrate described across the Mickai ebook series.

Profiles and links

mickai.co.uk · the canonical Mickai site.

crunchbase.com/person/micky-irons · founder profile.

linkedin.com/in/mickyirons · personal LinkedIn.

github.com/Micky-CMO · open-source position.

linkedin.com/company/mickai · Mickai LTD company page.

crunchbase.com/organization/mickyirons · Mickai LTD Crunchbase entry.

Email: press@mickai.co.uk

Colophon

Set in Inter Tight (Variable) and Inter Black. Brand voice audited under the Mickai AMT preflight gate; zero violations at publish.

References and further reading

· Nazrul Islam, 'AI's real workplace threat: surveillance and control', The Guardian, 11 May 2026.

· Information Commissioner's Office, workplace monitoring guidance, 2024 to 2025 series.

· UK GDPR Article 22, automated individual decision-making, including profiling.

· Trades Union Congress, digital workforce annual report, 2025 edition.

· Mickai OAR Brain documentation: mickai.co.uk/oar.

· Mickai trade mark UK00004373277, classes 9 and 42, filed 15 April 2026.