



JAOC INVESTIGATIONS



JAOC INVESTIGATION DOSSIER

POLICE SOCIAL MEDIA INTELLIGENCE:

AI Systems, Central Networks & Community Impact

— THE GLASGOW CONTEXT —

FOR PUBLIC RELEASE — IMMEDIATE

DISTRIBUTION: GENERAL PUBLIC

FOR INFORMATION, ADVICE & GUIDANCE PURPOSES

27 July 2026

© JAOC INVESTIGATIONS 2026 | www.jaoc.org.uk



DISCLAIMER & EXECUTIVE SUMMARY

DISCLAIMER

This dossier draws on publicly available documentation, official government publications, Freedom of Information disclosures, and independent research. Full algorithmic specifications, training datasets, and operational parameters of police AI systems remain classified or commercially sensitive. While every effort has been made to ensure accuracy, JAOC Investigations accepts no liability for any errors or omissions. Readers are encouraged to verify all claims through independent research. This document is issued for information, advice, and guidance purposes only. If any reader believes information herein to be incorrect, please contact JAOC Investigations via www.jaoc.org.uk.

EXECUTIVE SUMMARY

UK police forces are operating one of the most sophisticated social media intelligence architectures in the Western world – and the public knows almost nothing about it.

This dossier examines how automated systems and artificial intelligence gather, filter, and store social media intelligence; why this information is hidden from ordinary officers; and what this means for communities in Glasgow and across the United Kingdom.

The architecture is clear: public social media content is harvested via approved APIs and web crawlers, processed through AI triage systems, validated by analysts, and stored in central restricted repositories. But the opacity of AI decision-making, the profiling of children as young as 12, the disproportionate focus on ethnic minorities and young people, and the complete absence of public accountability raise fundamental questions about necessity, proportionality, and the erosion of civil liberties.

In Glasgow – one of the UK's most diverse cities – these systems are already having a chilling effect on lawful expression, political organising, and community solidarity. When "good people" are caught in broad sweeps, intelligence becomes unreliable, innocent reputations are harmed, and the very trust needed to keep communities safe is eroded.

THE QUESTION IS NO LONGER WHETHER THESE SYSTEMS EXIST.
THE QUESTION IS WHETHER WE, THE PEOPLE, WILL ALLOW THEM TO OPERATE IN THE DARK.



SECTION 1

THE COLLECTION & PROCESSING PIPELINE

1.1 WHAT IS HARVESTED

Only publicly available social media content is harvested via approved APIs and web crawlers.
Private data requires legal authorisation under RIPA 2000 and IPA 2016.

PLATFORMS MONITORED:

- X (formerly Twitter)
- Facebook
- TikTok
- Instagram
- YouTube
- Snapchat

KEY TOOLS AND SYSTEMS:

- FIVECAST – Social media screening and OSINT platform, approved for UK public sector use
- PROJECT ALPHA – Metropolitan Police intelligence-gathering initiative launched June 2019, employing 30 staff to monitor social media content including drill music videos
 - BEAT/PULSE – AI-enabled processing projects led by the Office of the Police Chief Scientific Adviser
- FORCE-SPECIFIC OSINT SYSTEMS – Individual police forces operate their own monitoring capabilities

1.2 THE AI TRIAGE LAYER

Once collected, data passes through an AI-enabled processing layer:

DEDUPLICATION	Removes duplicate content	May discard contextually distinct posts
CLASSIFICATION	Categorises content by risk	Bias in training data UNKNOWN
PATTERN-LINKING	Connects people, locations	"Suspicious by association" risk
ANOMALY DETECTION	Flags unusual behaviour	False positives on marginalised groups
SUMMARISATION	Condenses large volumes	Loss of nuance and context

CRITICAL GAP: The algorithms are opaque. There is no public scrutiny of training data, no independent bias testing, and no transparency about error rates.

The OPCS states: "AI does not replace human judgement... outputs are investigative leads, not conclusions." But if the AI layer is biased, the "leads" it generates are compromised from the outset.

1.3 ANALYST VALIDATION

A trained analyst must review all AI outputs before storage. However:

- Human oversight quality varies between forces
- Analysts work under pressure to process high volumes
- Confirmation bias means AI-flagged content is more likely to be validated
- There is no public accountability for validation errors



SECTION 2

CENTRAL RESTRICTED NETWORKS

Processed intelligence is held in tier-access repositories – NOT visible to general officers or the public.

2.1 POLICE NATIONAL DATABASE (PND)

Established: April 2011
Origin: Richard Inquiry (2004) following the Soham murders
Purpose: National intelligence sharing across all UK police forces
Data Held: "Soft intelligence" – allegations, suspicions, observations, custody details, domestic abuse reports, child protection records, OCG links
Scale: 53 data feeds, 200+ force databases consolidated, 12,000+ registered users
Classification: OFFICIAL-SENSITIVE to OFFICIAL-SENSITIVE HIGH
Access: Vetted analysts and investigators only – need-to-know basis

The PND is an intelligence data-handling system, NOT an evidential system. Records include allegations where no caution or conviction resulted. This "soft" information can appear on Enhanced DBS certificates, affecting employment prospects without any finding of guilt.

2.2 LAW ENFORCEMENT DATA SERVICE (LEDS)

Purpose: Replacing the Police National Computer (PNC, 1974–2026)
Status: Dual-running with PNC until March 2026 decommission
Data Held: Evidential records: arrests, charges, convictions, wanted persons
Scale: ~14 million Person records | ~75 million Vehicle records
~64 million Driver records
Transactions: 192+ million per year
Organisations: 150+ connected, including 127 non-police organisations
Access: Authorised frontline officers + approved third parties

LEDS is cloud-native, API-driven, and mobile-accessible. The Crime and Policing Act 2026 will expand driver licence data access to ANY policing or law enforcement purpose.

2.3 PoliceAI / NATIONAL HUBS

Function: AI-enabled processing layer for pattern-linking and predictive analytics
Capability: Automated suggested connections between people, objects, locations, events
Opacity: Training data, bias testing, and error rates are NOT publicly disclosed
Access: Specialist AI units and national intelligence hubs ONLY

WHY RESTRICTED? The official justification is DPA 2018/GDPR compliance, investigative sensitivity, and prevention of misuse. The practical effect is that communities cannot see, challenge, or correct what is held about them.



SECTION 3

LEGAL & GOVERNANCE FRAMEWORK

3.1 PRIMARY LEGISLATION

RIPA 2000 / IPA 2016	Rules for surveillance, authorisation, and oversight
DPA 2018 / UK GDPR	Data minimisation, fairness, retention, accountability
Police Act 1996 (amended)	Powers for national policing data systems
Crime and Policing Act 2026	Expands law enforcement data access powers

3.2 OPERATIONAL STANDARDS

College of Policing APP	Intelligence management, OSINT standards, audit trails
PNC/LEDS Code of Practice	10 principles for ethical and professional data use
Management of Police Information	National standards for police information management (MOPI 2021)

3.3 OVERSIGHT BODIES

BODY	ROLE	LIMITATION
IPCO	Monitors surveillance authorisations	Limited public reporting
ICO	Data protection enforcement	Reactive, under-resourced
HMICFRS	Police effectiveness & legitimacy	No power to halt programmes
Parliamentary	Legislative oversight	Often retrospective
	Scrutiny	

THE GOVERNANCE GAP: While oversight bodies exist, they are reactive, under-resourced, and lack the technical expertise to scrutinise AI systems effectively.

The College of Policing states that "access must be role-based, vetted, audited and removed when no longer needed" – but there is no independent verification that this happens in practice.

- KEY STATISTICS (2024–2026)
- 192M+ PNC transactions per year
 - 14M+ Person records on LEDS
 - 12,000+ PND registered users
 - 1,600+ child LFR watchlist inclusions
 - 30+ staff on Project Alpha
 - 150+ organisations connected to LEDS



SECTION 4

THE GLASGOW SITUATION

Glasgow – Scotland's largest city and one of its most diverse – is experiencing the sharp end of this surveillance architecture.

4.1 PROFILING & DISPROPORTIONATE FOCUS

GOVANHILL: CCTV coverage has put this multicultural area under 24-hour police surveillance since 2015. Community members report feeling "under the microscope."

PROJECT ALPHA: FOI disclosures reveal large-scale profiling of children as young as 13. Drill music videos are targeted for "intelligence gathering."

LIVE FACIAL RECOGNITION (LFR): Children as young as 12 have been included on police facial recognition watchlists. South Wales Police alone has included 632 under-18s since 2022. The College of Policing warns that facial recognition is LESS ACCURATE for children under 13 and "may lead to more false alerts."

4.2 SOLIDARITY & ACTIVISM SUPPRESSION

- Palestine solidarity events in Glasgow have been monitored and logged
- Copwatching initiatives – community-led police accountability projects – have been flagged in intelligence databases
- The Red Pepper investigation "From Scotland to Gaza: Solidarity Through Copwatching" documents how legitimate political expression is treated as suspicious

4.3 THE TRANSPARENCY GAP

Communities in Glasgow cannot know:

- What criteria are used to flag their social media posts
 - How AI systems judge "risk" or "anomaly"
 - How errors are corrected
 - How long data is retained
- Whether their names appear in PND or LEDS records

As the Open Rights Group notes:

"Large-scale systematic profiling... of children... raises fundamental questions about necessity and proportionality."



SECTION 5

COMMUNITY IMPACT ANALYSIS

5.1 THE CHILLING EFFECT

When people believe they are under surveillance, they change their behaviour – even when their actions are entirely lawful.

LAWFUL EXPRESSION	Self-censorship of political opinions online
POLITICAL ORGANISING	Fear of being flagged and logged deters participation
COMMUNITY SOLIDARITY	Reluctance to show support for controversial causes
INFORMATION SHARING	Withholding news, warnings, and advice
TRUST IN POLICE	Eroded by secret profiling and lack of accountability
YOUTH ENGAGEMENT	Children learn early that their digital footprint is policed

5.2 UNINTENDED CONSEQUENCES

When "good people" are caught in broad sweeps:

- Intelligence becomes unreliable (garbage in, garbage out)
 - Innocent reputations are permanently harmed
 - Willingness to assist police diminishes
 - Community cohesion fractures
 - Public safety is ultimately weakened

As Naked City Magazine observes:

"The more people feel they are under the microscope without justification, the less likely they are to cooperate or speak up."

5.3 THE KEY QUESTION

If AI triage is opaque and human oversight variable, how can communities be assured they are not being treated as "SUSPICIOUS BY ASSOCIATION"?

The answer, currently, is: they cannot.

The architecture is designed to be invisible. The data is classified. The algorithms are proprietary. The oversight is toothless. And the people being watched have no mechanism to know what is held about them, let alone challenge it.

This is not public safety. This is the architecture of control – built in plain sight, hidden behind comforting language, and funded by the very people it watches.



SECTION 6

HISTORICAL CONTEXT — WHEN THE PEOPLE ROSE

Throughout history, ordinary people have stood against controlling states and generated movements that changed the world.

The thread that binds them is simple: LAW IS NOT THE SAME THING AS JUSTICE, and a government that conflates the two is asking you to outsource your conscience to whoever currently holds office.

THE BOSTON TEA PARTY — 1773

"The People should never rise, without doing something to be remembered — something notable and striking." — John Adams, December 17, 1773
Colonists rejected taxation without representation. 342 chests of tea dumped into Boston Harbor. It was illegal. It was also the spark that lit a revolution.

HENRY DAVID THOREAU — 1849

"Under a government which imprisons any unjustly, the true place for a just man is also a prison."
Thoreau refused to pay a poll tax funding the Mexican War. He sat in jail rather than fund imperial violence. His essay "Civil Disobedience" inspired Gandhi, King, and every nonviolent resister since.

MAHATMA GANDHI & THE SALT MARCH — 1930

"You assist an evil system most effectively by obeying its orders and decrees. An evil system never deserves such allegiance."
A 240-mile march to make salt from seawater. 60,000 arrested. The British Empire began to crumble — not from violence, but from millions refusing to comply.

MARTIN LUTHER KING JR. — 1963

"One has a moral responsibility to disobey unjust laws." — Letter from Birmingham Jail
King deliberately broke unjust segregation laws and accepted arrest. He wrote the most important letter on civil disobedience in history from a Birmingham jail cell.

VÁCLAV HAVEL — 1978

"The power of the powerless is living within the truth." — The Power of the Powerless
Under total communist surveillance, Havel refused to participate in state rituals. He wrote samizdat essays. Eleven years later, he was President of Czechoslovakia.

FREDERICK DOUGLASS — 1857

"Power concedes nothing without a demand. It never did and it never will."
Escaped slavery. Became the most photographed American of the 19th century.
His message: "Knowledge makes a man unfit to be a slave."



SECTION 7

CONCLUSION & CALL TO ACTION

7.1 THE PRESENT MOMENT

We stand at a crossroads. The UK now operates:

- AI systems that profile children from age 12
- National databases holding "soft intelligence" on millions of innocent people
 - Facial recognition watchlists with no transparency
 - Social media monitoring that treats lawful expression as suspicious
- A governance framework that is reactive, under-resourced, and technically outmatched

The architecture of control is being built in plain sight – but hidden in plain sight, too. Hidden behind "need-to-know" access controls. Hidden behind commercially sensitive algorithms. Hidden behind the comforting language of "public safety."

7.2 THE COMING TOGETHER

This dossier calls for the COMING TOGETHER of like-minded people with a clear, coherent plan for a consistent message across social media networks.

We must be smarter than the people in government who restrict our freedoms. We must remember those in our history who stood up against the controlling state and generated movements of people, for the people.

MORE INFORMATION WILL FOLLOW. But for now, the plan is clear:

1. EDUCATE – Share this dossier. Make the invisible visible.
2. ORGANISE – Connect with others who value liberty over surveillance.
3. RESIST – Refuse to self-censor. Speak the truth, even when algorithms are listening.
4. DEMAND – Insist on transparency, accountability, and the right to know what is held about you.

7.3 THE FINAL WORD

"The spirit of resistance to government is so valuable on certain occasions, that I wish it to be always kept alive." – Thomas Jefferson, 1787

"There may be times when we are powerless to prevent injustice, but there must never be a time when we fail to protest." – Elie Wiesel, Nobel Peace Prize Lecture, 1986

When the machinery of the state is pointed at the powerless to protect the comfortable, the question stops being whether disobedience is permissible – and starts being whether COMPLIANCE IS.

WE ARE THE PEOPLE. WE HAVE THE NUMBERS. WE HAVE THE TRUTH.
AND WE WILL NOT BE SILENCED.



QUOTABLE REFERENCES

& FULL SOURCE LIST

QUOTABLE REFERENCES

"AI does not replace human judgement... outputs are investigative leads, not conclusions, requiring review, corroboration and assessment."
– Office of the Police Chief Scientific Adviser, BEAT Project

"Access must be role-based, vetted, audited and removed when no longer needed."
– College of Policing, PNC/LEDS Code of Practice

"Large-scale systematic profiling... of children... raises fundamental questions about necessity and proportionality."
– Open Rights Group, Project Alpha DPIA Analysis

"The more people feel they are under the microscope without justification, the less likely they are to cooperate or speak up."
– Naked City Magazine, Glasgow Intelligence Culture

FULL SOURCE LIST

1. GOV.UK (2026) Police use of artificial intelligence factsheet
2. College of Policing (2025) Intelligence Management APP
3. NPCC (2023) Guidance on Open Source Investigation/Research
4. Fivecast (2026) Social Media Screening Capabilities Framework
5. Office of the Police Chief Scientific Adviser (2025) BEAT/PULSE Project Summary
6. Open Rights Group (2022) Project Alpha DPIA Review
7. ICO / IPCO – Guidance on AI & Surveillance Law
8. The Guardian (2022) Met police profiling children on a large scale
9. Red Pepper (2026) From Scotland to Gaza: solidarity through copwatching
10. Naked City Magazine (2026) Rise of the Supergrasses
11. GOV.UK (2024) Police National Database 1.5 Transformation: Accounting Officer Assessment
12. GOV.UK (2026) Law Enforcement Data Service (LEDS) Data Protection Impact Assessment
13. Liberty Investigates / The Times (2025) Police forces use facial recognition to track children
14. Morning Star (2025) Met police collecting children's personal data
15. Police National Database Code of Practice (2010)
16. Privacy International – UK Law Enforcement Data Service (LEDS)
17. Glasgow Times (2015) CCTV to be installed in crime-hit Govanhill

END OF DOSSIER

© JAOC INVESTIGATIONS 2026

www.jaoc.org.uk

FOR PUBLIC RELEASE – IMMEDIATE

FOR INFORMATION, ADVICE & GUIDANCE PURPOSES ONLY