

← Executive Summary - TRUST Ordinance

Jesse Brown

Councilor, District 13

Indianapolis-Marion County City-County Council



MEMORANDUM

TO: Members of the Indianapolis-Marion County City-County Council

FROM: City-County Councilor Jesse Brown, District 13

DATE: September 12, 2026

SUBJECT: Comprehensive Legislative Package: Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance & Companion Oversight Resolution

Executive Summary

As public safety agencies increasingly rely on advanced digital tools, the City of Indianapolis must establish clear legislative guardrails to balance public safety needs with civil liberties, constitutional privacy, and fiscal accountability.

This legislative package introduces two complementary enactments:

- 1. TRUST Ordinance (General Ordinance):** Establishes mandatory City-County Council approval before municipal agencies or the Indianapolis Metropolitan Police Department (IMPD) acquire, fund, or deploy surveillance technologies. It mandates public Privacy Impact Assessments (PIAs), Surveillance Use Policies (SUPs), strict 30-day data retention caps, annual efficacy audits, and citizen enforcement remedies.
 - 2. Companion Resolution:** Establishes the Public Surveillance and Technology Oversight Board (PSTOB), a 9-member independent resident body tasked with reviewing technology impact proposals, conducting public hearings, and advising the Council.
-

← Executive Summary - TRUST Ordinance

- **Democratic Oversight & Transparency:** Shifts acquisition authority from administrative procurement directly to the elected representatives on the City-County Council through mandatory public hearings.
- **Civil Liberties & Constitutional Safeguards:** Limits bulk data collection, prohibits third-party vendor monetization of local data, and ensures clear access logging to protect Fourth Amendment rights.
- **Targeted Retention & Accountability:** Prevents indefinite state data storage by enforcing default deletion of non-evidentiary data after 30 days while mandating annual reporting on clear rates, false positives, and total operating costs.
- **Legal Resilience:** Includes a robust severability clause and a "springing reenactment" provision designed to protect local authority and instantly reactivate provisions should state preemption laws be altered or struck down.

Key Legislative Components

Component	TRUST Ordinance	Oversight Board Resolution
Primary Function	Sets legal standards, binding Council approval rules, retention limits, and private right of action.	Establishes an independent resident advisory board to vet technology proposals and host public hearings.
Governance Structure	City-County Council vote required for all acquisitions, scope expansions, or data-sharing agreements.	9-member board (4 Council appointees, 4 Mayoral appointees, 1 Public Defender appointee).
Mandatory Filings	Public Privacy Impact Assessments (PIAs) and Surveillance Use Policies (SUPs) required 30 days prior to vote.	Formal written recommendations issued to Council within 45 days of document receipt.
Exigent Use Rule	Emergency deployment allowed only for imminent threats; retro-approval required within 14 days.	N/A
Enforcement	Injunctions, data purges, statutory damages (\$1,000/violation), and whistleblower protections.	Annual compliance audits reported directly to Council and City Legal Division.

← Executive Summary - TRUST Ordinance

CITY OF INDIANAPOLIS / MARION COUNTY

PROPOSED LEGISLATIVE PACKAGE: SURVEILLANCE TECHNOLOGY OVERSIGHT & TRANSPARENCY

PART I: CONSOLIDATED ORDINANCE

CITY-COUNTY COUNCIL GENERAL ORDINANCE NO. ____, 2026

Title: Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance

Purpose: To establish public oversight, transparency, civil liberties protections, and City-County Council approval requirements prior to the acquisition, funding, deployment, or operational expansion of surveillance technology by Indianapolis-Marion County municipal agencies and the Indianapolis Metropolitan Police Department (IMPD).

Section 1. Definitions

- **Surveillance Technology:** Any electronic device, system, algorithm, or software designed or primarily used to monitor, collect, retain, analyze, process, or share audio, visual, location, thermal, biometric, or digital data of individuals or groups.
 - *Includes:* Automated License Plate Readers (ALPRs), facial recognition software, aerial drones, cell-site simulators, predictive policing algorithms, gunshot detection systems (e.g., ShotSpotter), and integrated public/private video feeds.
 - *Excludes:* Routine office technology (email servers, standard IT security firewalls), internal employee badge readers, and traffic-signal timing sensors that do not store or track identifiable video/data.
- **Sensitive Personal Information:** Data revealing precise real-time or historical geolocation, biometric traits, genetic information, religious affiliations, political activities, trade union memberships, or the contents of private communications.

Section 2. City-County Council Approval Requirement No Indianapolis-Marion County department, agency, or law enforcement entity (including IMPD) shall take any of the following actions without prior approval by a majority vote of the City-County Council via full public hearing:

← Executive Summary - TRUST Ordinance

- Deploying existing surveillance technologies for purposes or operational scopes not previously authorized by the Council.
- Entering into data-sharing agreements with third-party vendors, state/federal law enforcement agencies, or private security networks.

Section 3. Mandatory Impact Documents At least 30 days prior to Council consideration of any surveillance technology proposal, the proposing agency must publish the following documents to the public city portal:

1. Privacy Impact Assessment (PIA):

- Analysis of potential risks to Fourth Amendment protections, privacy rights, and civil liberties.
- Evaluation of disproportionate impacts on historically marginalized communities or protected classes.
- Assessment of alternative, less invasive technology options to achieve the stated public safety goal.
- Prohibition on third-party vendor monetization, machine-learning training on City data, or secondary commercial distribution of collected data.

2. Surveillance Use Policy (SUP):

- **Authorized Uses:** An explicit, non-exhaustive list of approved operational scenarios.
- **Data Retention & Deletion:** Strict retention caps (maximum 30-day default retention unless flagged as evidence in an active criminal investigation).
- **Access Protocols:** Role-based access controls detailing exactly who can view or export data.
- **Auditing:** System logging requirements for every database search, including mandatory case number entry for audit trails.

Section 4. Exigent Circumstances & Legacy Systems

- **Exigent Circumstances:** Emergency deployment without prior approval is permitted only during a declared state of emergency or an imminent threat of death or serious physical injury. Public

← Executive Summary - TRUST Ordinance

- **Existing Technologies.** Technologies deployed prior to the enactment of this ordinance must submit a PIA and SUP to Council within 180 days to maintain operating authorization.

Section 5. Oversight & Annual Reporting By March 1 of each calendar year, the City Controller and IMPD Chief of Police must present an annual public report detailing:

- Total operating and maintenance costs for each active surveillance technology.
- Quantitative efficacy metrics (e.g., arrest connections, clear rates, false-positive frequencies).
- Records of compliance audits, data breaches, unapproved access attempts, or disciplinary actions taken for unauthorized use.

Section 6. Enforcement, Private Right of Action, and Citizen Remedies

- **(a) Right of Action:** Any resident of Marion County or individual subjected to surveillance in violation of this Ordinance may bring a civil action in a court of competent jurisdiction against the City of Indianapolis, Marion County, or the responsible municipal agency.

- **(b) Remedies:** Upon proof of a violation, the court shall grant:

1. *Injunctive Relief:* Mandatory temporary or permanent injunctions requiring the immediate cessation of unauthorized surveillance, shutdown of data collection systems, and complete purge of unlawfully collected data.

2. *Declaratory Relief:* A judicial order declaring the deployment, data-sharing agreement, or contract null and void.

3. *Statutory Damages:* Liquidated damages of \$1,000 per violation or \$100 per day of unauthorized deployment, whichever is greater, payable to the prevailing plaintiff.

4. *Attorneys' Fees:* Award of reasonable attorneys' fees and litigation costs to a prevailing plaintiff.

- **(c) Whistleblower Protections & Audits:** City employees or IMPD officers reporting unauthorized surveillance shall be protected under local and state whistleblower laws. The City Controller shall initiate a 30-day mandatory audit upon receiving any credible report of non-compliance.

Section 7. Severability, Interdependence, and Reactivation

- **(a) General Severability:** If any provision of this Ordinance is held unconstitutional, preempted by

← Executive Summary - TRUST Ordinance

• **(b) Severability of Companion Resolution.** Invalidation or preemption of City-County Council Resolution No. ____, 2026 (establishing the Oversight Board) shall not diminish the enforcement of this Ordinance. Departmental reporting, PIAs, SUPs, annual audits, and Council prior approval requirements shall remain in full force and submit directly to the City-County Council.

• **(c) Springing Reenactment:** Should any provision be preempted or invalidated by state statute or judicial decree, and such statute or decree is subsequently repealed, amended, or overturned, the affected provisions shall automatically regain full legal force and effect without requiring further legislative action.

• **(d) Legislative Intent:** The City-County Council declares it would have passed this Ordinance and its companion resolution independently, irrespective of any judicial or legislative invalidation of specific sections.

PART II: COMPANION RESOLUTION

CITY-COUNTY COUNCIL RESOLUTION NO. ____, 2026

Title: A Resolution Establishing the Public Surveillance and Technology Oversight Board (PSTOB)

Purpose: To create an independent, resident-led advisory board tasked with evaluating surveillance technology proposals, conducting privacy reviews, and providing community oversight regarding the implementation of the TRUST Ordinance.

Section 1. Establishment and Composition

• **Establishment:** There is hereby established the Public Surveillance and Technology Oversight Board (PSTOB).

• **Membership:** Nine (9) voting Marion County residents:

- **Four (4) appointments** by the City-County Council (at least two representing civil liberties, racial justice, or privacy organizations).
- **Four (4) appointments** by the Mayor of Indianapolis (one with cybersecurity/data privacy expertise; one with a background in public safety or law enforcement ethics).
- **One (1) appointment** selected by the Marion County Public Defender Agency.

← Executive Summary - TRUST Ordinance

consecutive terms) without compensation.

Section 2. Powers and Duties

- **Review Impact Documents:** Evaluate all PIAs and SUPs prior to Council submission.
- **Public Hearings:** Host at least one mandatory public hearing for every proposed surveillance acquisition or operational modification.
- **Written Recommendations:** Issue formal written recommendations to the City-County Council within 45 days of receiving a complete PIA and SUP.
- **Annual Audit Review:** Analyze annual surveillance reports, assess SUP compliance, and report material non-compliance directly to the Council and City Legal Division.
- **Policy Recommendations:** Propose updates, stricter privacy safeguards, or sunset provisions for existing technologies as capabilities evolve.

Section 3. Staffing and Resources

- **Administrative Support:** Office of Corporation Counsel and City-County Council staff shall provide administrative and legal support.
- **Access to Information:** City departments and IMPD shall provide non-confidential operational information, system specifications, and access log samples required for oversight duties.

As always, I am happy to work with any colleagues to answer questions, address concerns, or add anyone as a cosponsor of this legislation.

Thanks for considering!

In love and solidarity,
Jesse



Jesse Brown
City-County Council, District 13
Cell: 317-370-7079
Email: jesse@jesseforindy.com