CITY OF URBANA
COMMITTEE OF THE WHOLE MEETING

DATE: Tuesday, September 02, 2025
TIME: 7:00 PM
PLACE: 400 South Vine Street, Urbana, IL 61801

AGENDA

Chair: ***James Quisenberry, Ward 7***

A. Call to Order and Roll Call

B. Approval of Minutes of Previous Meeting

C. Additions to the Agenda

D. Presentations and Public Input

1. **Transforming the City-owned Parking Lot North of the Rose Bowl into a Permanent Plaza - CM's Evans and Wilken**

E. Staff Report

F. New Business

G. Discussion

1. **Police Surveillance Technology (Ordinance No. 2024-12-042)**

H. Council Input and Communications

I. Adjournment

All City meetings are broadcast on Urbana Public Television and live-streamed on the web. Details on how to watch are found on the UPTV webpage located at https://www.urbanail.gov/executive-department/page/urbana-public-television.

PUBLIC INPUT

The City of Urbana welcomes Public Input during open meetings of the City Council, the City Council's Committee of the Whole, City Boards and Commissions, and other City-sponsored meetings. Our goal is to foster respect for the meeting process, and respect for all people participating as members of the public body, city staff, and the general public. The City is required to conduct all business during public meetings. The presiding officer is responsible for conducting those meetings in an orderly and efficient manner. Public Input will be taken in the following ways:

Email Input
Public comments must be received prior to the closing of the meeting record (at the time of adjournment unless otherwise noted) at the following: citycouncil@urbanail.gov. The subject line of the email must include the words "PUBLIC INPUT" and the meeting date. Your email will be sent to all City Council members, the Mayor, City Administrator, and City Clerk. Emailed public comments labeled as such will be incorporated into the public meeting record, with personal identifying information redacted. Copies of emails will be posted after the meeting minutes have been approved.

Written Input
Any member of the public may submit their comments addressed to the members of the public body in writing. If a person wishes their written comments to be included in the record of Public Input for the meeting, the writing should so state. Written comments must be received prior to the closing of the meeting record (at the time of adjournment unless otherwise noted).

Verbal Input
Protocol for Public Input is one of respect for the process of addressing the business of the City. Obscene or profane language, or other conduct that threatens to impede the orderly progress of the business conducted at the meeting is unacceptable.

Public comment shall be limited to no more than five (5) minutes per person. The Public Input portion of the meeting shall total no more than two (2) hours, unless otherwise shortened or extended by majority vote of the public body members present. The presiding officer or the city clerk or their designee, shall monitor each speaker's use of time and shall notify the speaker when the allotted time has expired. A person may participate and provide Public Input once during a meeting and may not cede time to another person, or split their time if Public Input is held at two (2) or more different times during a meeting. The presiding officer may give priority to those persons who indicate they wish to speak on an agenda item upon which a vote will be taken.

The presiding officer or public body members shall not enter into a dialogue with citizens. Questions from the public body members shall be for clarification purposes only. Public Input shall not be used as a time for problem solving or reacting to comments made but, rather, for hearing citizens for informational purposes only.

In order to maintain the efficient and orderly conduct and progress of the public meeting, the presiding officer of the meeting shall have the authority to raise a point of order and provide a verbal warning to a speaker who engages in the conduct or behavior proscribed under "Verbal Input". Any member of the public body participating in the meeting may also raise a point of order with the presiding officer and request that they provide a verbal warning to a speaker. If the speaker refuses to cease such conduct or

behavior after being warned by the presiding officer, the presiding officer shall have the authority to mute the speaker's microphone and/or video presence at the meeting. The presiding officer will inform the speaker that they may send the remainder of their remarks via e-mail to the public body for inclusion in the meeting record.

Accommodation

If an accommodation is needed to participate in a City meeting, please contact the City Clerk's Office at least 48 hours in advance so that special arrangements can be made using one of the following methods:

- Phone: 217.384.2366
- Email: CityClerk@urbanail.gov

Department	Database or Tool	Owner or Vendor	Purpose
CD	Third-party data analysis from cellphone usage	Placer.ai	Placer uses anonymized cell data, and only uses location data provided by apps that people have opted into allowing (i.e. individuals have opted in to allow location services for the app). That seems to exclude Placer from Defition 1, 4.a.8, which describes GPS data collection *without authorization.*
UFD	Drones (never operationalized)	Urbana Fire Department	Our drone program was never actually operational. The intent was to use these at large scale incidents for a higher-level view of the entire incident and better point of vantage to see the progression of the incident, training, size ups, and search and rescue operations. We are also interseted in a drone first responder program that could allow us to see incidents before the arrival of our apparatus which could potentially help us reduce our response package.
PW	Miovision	Miovision	Traffic data for intersection and corridor studies.
PW	Streetlight	Hanson (consultant)	GPS data from cell phones, connected vehicles, and other data sources for traffic movements, traffic volumes, and speed traveled. Presumably de-identified.
PW	City of Urbana asset tracking technology	OpenGov Enterprise Asset Management	GPS tracking (vehicles, phones, tablets, etc.).
PW	Contract recycling technology	GFL Enviornmental Inc.	Contractor utilizes technology that tracks their location and street view to eliminate discrepancies between calls for missed services versus failure of users to place cans out timely.
PW	Third-party data analysis from cellphone usage	For example, Placer.ai	GPS data for traffic information (includes Placer.ai)
PW	Drone footage	CUMTD	Typically used for community promotion and/or marketing pre/post conditions related to capital improvement projects. CUMTD has a drone and has provided assistance with this on projects like Florida Avenue (for RAISE grant), Fire Stations, PW Campus Rehab, as well as the Market at the Square Parking Lot Mural.
HR/F	Third-party administrators of worker's compensation cases	Contracted by a third party	Related to workers comp cases. This could be used in a workers comp proceeding, which would fall under the “criminal and civil action” category. Generally this is done mostly through observation by an investigator, not using specific surveillance technology.
IT	Outlook (electronic mail and calendar)	Microsoft, Intradyn, Barracuda	1) I would argue anyone emailing a City official or employee does not have a reasonable expectation of privacy in that communication. 2) We are required by law to inventory and retain email communications to comply with record keeping requirements *[and FOIA]* . I agree that including email in "manually operated" seems unusual.
IT	Cybersecurity tools	Microsoft, Barracuda, Blueshift, Cloudflare (State of IL DoIT), Duo, Okta	*"Cybersecurity software is designed to protect digital systems and data from unauthorized access, malicious attacks, ransomware, and theft. Its purpose is to safeguard sensitive information, ensure continuity, and maintain trust." IT is concerned about moving "decisions about sensitive and high-risk subject matter one additional degree of separation from the subject matter experts".*
UPD	ARCOS (Automation of Reports and Consolidated Orders System)	DEA	Tracks distribution of controlled substances from manufacturers to distributors.
UPD	ASEANAPOL Database	ASEANAPOL	Facilitates intelligence sharing among ASEAN police forces.
UPD	ATF E-Trace	Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)	Traces firearms recovered in crimes to their source.
UPD	ATS (Automated Targeting System)	Department of Homeland Security (DHS)	Analyzes risk and targets in customs and border protection.
UPD	ByteDance	ByteDance Inc.	Parent company of TikTok; may be listed due to data privacy concerns.
UPD	CA-PPT (Consular Affairs Passport Database)	U.S. Department of State	Manages passport application and issuance records.
UPD	CCD (Consular Consolidated Database)	U.S. Department of State	Consolidates visa and passport information for U.S. citizens and foreign nationals.
UPD	CLEAR (by Thomson Reuters)	Thomson Reuters	Investigative database providing public records and analytics.
UPD	CODIS (Combined DNA Index System)	FBI	Links DNA profiles from crime scenes and offenders.
UPD	Carfax for Police	Carfax Inc.	Provides vehicle history reports and investigative data to police.
UPD	Champaign County Warrants Database	Champaign County	Tracks active warrants issued in Champaign County.
UPD	Concealed Carry License Database	Illinois State Police	Stores data on licensed concealed carry holders in Illinois.
UPD	Cook County Government	Cook County	County government entity; may manage legal and corrections systems.
UPD	Cook County Integrated Criminal Justice Information System	Cook County	Platform for court and criminal justice data integration.
UPD	CrowdTangle	Facebook (Meta)	Tracks engagement and content performance on social media.
UPD	Dataminr	Dataminr Inc.	Real-time alerting and social media signal monitoring platform.
UPD	DepartmentWare	City of Urbana	City employee/department management and workflow system.
UPD	DHS (Department of Homeland Security)	U.S. Department of Homeland Security	Federal agency overseeing national security and immigration enforcement.
UPD	DuckDuckGo	DuckDuckGo Inc.	Privacy-focused search engine; may be monitored by surveillance tools.
UPD	El Paso Intelligence Center (EPIC)	DEA	Fusion center coordinating federal, state, and local intelligence sharing.
UPD	Envisage Technologies	Envisage Technologies	Training and compliance software vendor for public safety agencies.

UPD	European Union	European Union	Intergovernmental body; EU partner in criminal justice cooperation.
UPD	Europol Information System (EIS)	Europol	Database for sharing intelligence among European law enforcement.
UPD	Facebook	Meta Platforms, Inc.	Social media platform used for open-source investigations.
UPD	Geofeedia	Geofeedia Inc.	Social media analytics tool for geolocation and trend tracking.
UPD	Google	Google LLC	Search engine often used in investigations and intel gathering.
UPD	HSIN (Homeland Security Information Network)	Department of Homeland Security (DHS)	Secure information-sharing system for homeland security.
UPD	IAFIS (Integrated Automated Fingerprint Identification System)	FBI	Centralized fingerprint identification system.
UPD	ICJIA Data Portal	Illinois Criminal Justice Information Authority (ICJIA)	State-level criminal justice data and research platform.
UPD	IDENT (Automated Biometric Identification System)	Department of Homeland Security (DHS)	Biometric identification system for DHS.
UPD	IDIcore	IDI, Inc.	Investigative data provider offering public record analysis.
UPD	Illinois Amber Alert System	Illinois State Police	Search for state prison inmates and case info.
UPD	Illinois Department of Corrections Inmate Search	IDOC	Ticket issuance and tracking system for law enforcement.
UPD	Illinois eCitation Program	Illinois State Police	Terrorism intelligence and information-sharing hub in Illinois.
UPD	Illinois Statewide Terrorism and Intelligence Center (STIC)	Illinois State Police	Notifies victims about status changes in criminal cases.
UPD	Illinois Automated Victim Notification System (AVN)	Illinois Attorney General / IDOC	Image and video-sharing platform monitored in investigations.
UPD	Instagram	Meta Platforms, Inc.	Social media platform used for open-source investigations.
UPD	Interpol 24/7	Interpol	Illinois' centralized law enforcement data system.
UPD	LEADS (Law Enforcement Agencies Data System)	Illinois State Police	Public records search tool used in investigations.
UPD	LexisNexis Accurint	LexisNexis Risk Solutions	Professional networking platform with OSINT uses.
UPD	LinkedIn	Microsoft	Social media platform used for open-source investigations.
UPD	Lost and Stolen Passport Database	U.S. Department of State	Identifies missing and unidentified persons.
UPD	NamUs (National Missing and Unidentified Persons System)	U.S. Department of Justice / NIJ	Narcotics and drug trafficking investigations database.
UPD	NADDIS (Narcotics and Dangerous Drugs Information System)	DEA	Nationwide criminal history and warrant database.
UPD	NCIC (National Crime Information Center)	FBI	Ballistics imaging to link firearms to crimes.
UPD	NIBIN (National Integrated Ballistic Information Network)	ATF	Tracks detailed data on criminal incidents.
UPD	NIBRS (National Incident-Based Reporting System)	FBI	Shares crime-related data between jurisdictions.
UPD	N-DEx (National Data Exchange)	FBI	License plate and violation analytics system (unclear source).
UPD	Platelogix	Possibly PlateLogix Inc.	Tracks persons of interest across EU member states.
UPD	Schengen Information System (SIS)	European Union / Schengen States	Manages foreign students and visa holders in U.S.
UPD	SEVIS (Student and Exchange Visitor Information System)	U.S. Department of Homeland Security (DHS)	Searches exposed internet-connected devices and networks.
UPD	Shodan	Shodan LLC	Archives state communications and digital records.
UPD	SMART (State Messaging and Archive Retrieval Toolset)	Illinois State Archives / CMS	Captures and preserves social media for evidentiary use.
UPD	Social Media Analysis Tools (e.g., X1 Social Discovery)	X1 Discovery Inc.	Tracks cross-border movements and customs violations.
UPD	TECS (Treasury Enforcement Communications System)	U.S. Department of Homeland Security (CBP)	Investigative platform for people and businesses.
UPD	TLOxp (by TransUnion)	TransUnion	Crime statistics reporting system.
UPD	UCR (Uniform Crime Reporting Program)	FBI	Tracks violent serial offenders across jurisdictions.
UPD	VICAP (Violent Criminal Apprehension Program)	FBI	Access program database for U.S. State Dept. guests.
UPD	Wayback Machine (Internet Archive)	Internet Archive	Historical archive of websites and online content.
UPD	WLP (International Visitor Leadership Program Database)	U.S. Department of State	Sex offender registry for public notification.
UPD	Winols Sex Offender Registry	Illinois State Police	Video-sharing platform used for public content monitoring.
UPD	YouTube	Google LLC	Video-sharing platform used for public content monitoring.

CITY OF URBANA

City of Urbana
400 S. Vine Street, Urbana, IL 61801
www.urbanail.gov

MEMORANDUM TO THE MAYOR AND CITY COUNCIL

Meeting: September 2, 2025, Committee of the Whole
Subject: List of Technology and Databases for the Ordinance Establishing Approval, Policy, and Reporting Requirements for Surveillance Technology and Databases

---

Summary

Action Requested
To review the information provided.

Brief Background
The proposed ordinance outlines a framework to ensure that the City's use of surveillance technology and databases is transparent, accountable, and consistent with community expectations regarding privacy, civil liberties, and responsible governance. It establishes requirements for Council approval prior to the acquisition or deployment of such technology, sets standards for its use, and provides for regular reporting to City Council and the public.

Discussion

Additional Background Information
As part of the ordinance discussion, staff have prepared a document listing the surveillance technologies and databases currently in use by the City of Urbana. This inventory is intended to provide Council and the public with a clear picture of the tools presently in use.

It is important to note that the document provided does not represent a final or exhaustive list of all technologies and databases used by the City. This initial inventory will serve as a working document and will be updated as new information becomes available, additional technologies are identified, or new systems are adopted.

Recommendation
Staff recommend that Council review the attached ordinance and accompanying list of technologies and databases, understanding that the list is preliminary and will continue to be refined. Adoption of the ordinance will establish a consistent policy framework for Council oversight and community transparency in the City's use of surveillance technology and databases.

Attachments

1. All Depts Surveillance Tools

Originated by: Tarek Azim, Management Analyst and Darius White, City Administration

MEMORANDUM TO THE URBANA, IL COMMITTEE OF THE WHOLE & CITY COUNCIL

Meeting: May 19, 2025 Committee of the Whole

Subject: Ordinance No. 2024-12-042: An Ordinance Establishing Approval, Policy, and Reporting Requirements for Surveillance Technology and databases

Sponsors: Council Members Grace Wilken & Jaya Kolisetty

Summary

Action requested

City Council is asked to approve the attached Ordinance, which requires and clarifies the process for procurement and use of policing technology and databases that can be used to monitor, track, and identify specific individuals or groups. This Ordinance codifies the public approval process for specific surveillance technologies or databases; it does not dictate the use of any given technology (that would be voted on by Council).

Overall, the Ordinance establishes the Council approval and public input process for new and existing policing technologies and databases. The attached definitions clarify the relevant types of technology and databases, the Use Report, Use Policy, and Policing Technology Annual Report.

Brief Background & Previous Action

City of Urbana adopted the Ten Shared Principles on June 22, 2020 in Resolution No. 2020-06-031R which states "We reject discrimination toward any person that is based on race, ethnicity, religion, color, nationality, immigrant status, sexual orientation, gender, disability, or familial status;" provides support to "build and rebuild trust through procedural justice, transparency, accountability, and honest recognition of past and present obstacles" and advocates for "the four pillars of procedural justice, which are fairness, voice (i.e., an opportunity for citizens and police to believe they are heard), transparency, and impartiality"

City of Urbana reaffirmed its commitment as a sanctuary city in Resolution No. 2016-12-070R, stating that "the City Council and the Mayor will join with councils and mayors from other communities around the country to stand with our immigrant residents and defend policies that welcome and protect immigrants…" and that "no city employee or official or department or agency of the City of Urbana shall request information about or otherwise investigate or assist in the investigation of the citizenship or immigration status of any person unless such inquiry or the investigation is required by a court order…"

The City of Urbana commissioned the completion of a review of UPD and UFD policies and staffing requirements by Berry Dunn consultants. The report on the first phase of the study included community stakeholder meetings, professional stakeholder meetings, community interest group and individual meetings, and an online survey, all of which included responses from community members showing "a desire for more active transparency" (page 58). The report noted transparency as one of the four pillars of procedural justice and is included in the six pillars of 21st Century Policing, and that not providing transparency through community input "can foster mistrust and damage relationships" (page 159).

In, September of 2021, the Urbana City Council was asked to approve a budget amendment, allowing the City to move funds in order to purchase automatic license plate readers. After much discussion and public input, including Town Hall Meetings, the budget amendment failed, with a 4 to 3 vote, in November of 2021. This instance highlighted the fact that there was no procurement policy for police surveillance technology.

During the budget discussions in June of 2023, Council Members Wilken and Evans proposed additional language to the budget ordinance that clarified the intended use of approved funds and required Council approval and due public process for the purchase of certain surveillance technologies. That proposed language failed, with a 5 to 2 vote. There was feedback from Council members on how to improve the language, and comments that they would entertain a discussion about surveillance policy in the future.

In response to the proposed budget language, on the June 26, 2023 City Council meeting, Mayor Marlin stated that, "The city of Urbana will not authorize or purchase Automated License Plate Reader (ALPR) technology, without explicit majority approval from the Urbana City Council. While the prior debate and vote on ALPRs centered on a budget amendment to purchase ALPRs, rather than a general policy statement, the council discussion and 4-3 vote defeating the amendment, made the position of the majority of council very clear."

The attached Ordinance is a product inspired from years of discussion and thought in the Urbana community. The Ordinance is intended to simply codify the understanding by which the City has been operating for years, and define mechanisms public reporting. It has undergone some preliminary reviews, and continued feedback and collaboration is welcomed.

Financial Impact

There is no expected direct financial impact of this Ordinance.

Additional Information & Resources

Model Legislation from the Policing Project, New York University School of Law (this is similar to the originally proposed Ordinance):

https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5df2acb192c2512f27a73c12/1576185009882/ADAPT+Act.pdf

General resources on legislation for policing technology from the Policing Project:
https://www.policingproject.org/policing-technology-model-statutes-and-legislative-resources

Ordinance on surveillance technology from Boston, MA (these definitions were used for the updated Ordinance):
https://www.boston.gov/sites/default/files/file/2021/09/Docket%20%230397%20%282%29.pdf

Boston Police Department 2023 Annual Surveillance Technology Report:
https://www.boston.gov/sites/default/files/file/2024/07/2023%20City%20of%20Boston%20Annual%20Surveillance%20Reports_0.pdf

Oakland, CA Ordinance to amend the City Code regarding police surveillance:
https://cao-94612.s3.us-west-2.amazonaws.com/documents/OMC-9.64-January-2021-005.pdf

Oakland, CA Privacy Commission – other resources and ordinances:
https://www.oaklandca.gov/documents/privacy-advisory-board-ordinances-and-resolution

ACLU Community Control Over Police Surveillance (this is the same group that created the guiding principles that were attached in the packet for the December 16, 2024 Committee of the Whole meeting):
https://www.aclu.org/community-control-over-police-surveillance#:~:text=The%20proliferation%20in%20local%20police,color%20and%20low%2Dincome%20communities.

Research on data privacy and communities of color, from the Brookings Institution:
https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

ACLU article on the use of ALPR data by ICE (US Immigration and Customs Enforcement) to target people who have immigrated to the US, including in Illinois and in "sanctuary cities":
https://www.aclu.org/news/immigrants-rights/documents-reveal-ice-using-driver-location-data

Forbes article on lawsuits over license plate readers:
https://www.forbes.com/sites/larsdaniel/2024/10/22/warrantless-surveillance-federal-lawsuit-challenges-flock-safety-cameras/

ACLU model legislation: https://www.aclu.org/documents/community-control-over-police-surveillance-model-bill

Attachments

1. Ordinance No. 2024-12-042: An Ordinance Establishing Approval, Policy, and Reporting Requirements for Surveillance Technology and Databases (version 6)
2. Attachment A, Definitions (Ordinance No. 2024-12-042)

Ordinance No. 2024-12-042

AN ORDINANCE ESTABLISHING APPROVAL, POLICY, AND REPORTING REQUIREMENTS FOR SURVEILLANCE TECHNOLOGY AND DATABASES

WHEREAS, the City of Urbana ("City") is a home rule unit of local government pursuant to Article VII, Section 6, of the Illinois Constitution, 1970, and may exercise any power and perform any function pertaining to its government and affairs, and the passage of this Resolution constitutes an exercise of the City's home rule powers and functions as granted in the Illinois Constitution, 1970; and

WHEREAS, the City of Urbana reaffirmed its commitment as a sanctuary city in Resolution No. 2016-12-070R, stating that "the City Council and the Mayor will join with councils and mayors from other communities around the country to stand with our immigrant residents and defend policies that welcome and protect immigrants…" and that "no city employee or official or department or agency of the City of Urbana shall request information about or otherwise investigate or assist in the investigation of the citizenship or immigration status of any person unless such inquiry or the investigation is required by a court order…"; and

WHEREAS, the City of Urbana adopted the Ten Shared Principles on June 22, 2020 in Resolution No. 2020-06-031R which states "We reject discrimination toward any person that is based on race, ethnicity, religion, color, nationality, immigrant status, sexual orientation, gender, disability, or familial status;" provides support to "build and rebuild trust through procedural justice, transparency, accountability, and honest recognition of past and present obstacles" and advocates for "the four pillars of procedural justice, which are fairness, voice (i.e., an opportunity for citizens and police to believe they are heard), transparency, and impartiality"; and

WHEREAS, it is the Urbana City Council ("Council" or "City Council") and City's responsibility to legislate matters of public safety and accountability to the public, and any use or expense of surveillance technology or major systems regarding public safety require due public process and approval from City Council; and

WHEREAS, the Urbana City Council finds that no decision relating to surveillance technology should be made without collaborative community input and consideration of the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by Article I of the Illinois Constitution and the First, Fourth, and Fourteenth Amendments to the United States Constitution; and

WHEREAS, the use of surveillance technologies are known to have had a significant, detrimental impact on civil rights and civil liberties, namely the invasion of an individual's privacy and infringing on their right to be left alone, including those guaranteed by the First, Fourth and Fourteenth Amendments to the United States Constitution, and thus it is incumbent on the police or other agency seeking to fund, acquire, or use a surveillance technology to expressly identify the potential adverse impacts the technology may have on civil rights and civil liberties and what specific measures it will undertake to prevent such adverse impacts; and

WHEREAS, surveillance technologies can create oppressive, stigmatizing environments when used indiscriminately, continuously, or pervasively, especially for communities that have historically been disproportionately targeted by their use, such as communities of color, low income communities, and politically active communities; and

WHEREAS, the urgency to publicly process the acquisition of surveillance technologies is necessitated by new concerns whether surveillance technologies will be used to apprehend people from out-of-state seeking abortions and other reproductive healthcare in Illinois; people without legal immigration status who seek asylum and would be sought for deportation; peaceful individuals or organizations exercising their rights, including expressing grievances against the government; and people whose race, national origin, ethnic identity, gender identity, sexual orientation, or other protected demographics place them under potential for additional surveillance; and

WHEREAS, the need for a public process to acquire surveillance technologies is further required because of the likelihood that federal law enforcement agencies will access any data stored by surveillance technologies; and

WHEREAS, as of the passing of this ordinance, there is no current city policy on the use and acquisition of police surveillance technology, and it is therefore necessary to clarify the Council's position on the required processes of public accountability;

NOW THEREFORE BE IT ORDAINED by the City Council, of the City of Urbana, Illinois, as follows:

Section 1. Purpose:

The purpose of this ordinance is to provide transparency, oversight, and accountability regarding the acquisition and use of surveillance technology and surveillance data by the City of Urbana and all departments and officials (hereinafter "City" or "City Department"), and to protect privacy, civil rights, and racial and immigrant justice.

Section 2. Approval Process for Surveillance Technology and Database Acquisition or Use

(a) Any City Department seeking to acquire or use new surveillance technology or surveillance data, shall, prior to such acquisition or use obtain ~~written~~ approval by majority vote of the Urbana City Council prior to purchasing, acquiring, or using any new surveillance technology or database (as defined in Attachment A of this Ordinance), which includes linking or cross-referencing existing databases, adding new categories of data to a database, or using new analytic tools on an existing database.

(b) At least sixty (60) days prior to seeking approval of a surveillance technology or database, the City shall submit to the City Council and make publicly available a written and unredacted surveillance technology or database "Use Report," along with a draft of the proposed surveillance technology or database "Use Policy" (as defined in Attachment A of this Ordinance).

(c) The public shall have forty-five (45) days subsequent to filing of the surveillance technology or database "Use Report" and "Use Policy" to submit formal comments to the City Council.

Section 3. Standard for Approval of Surveillance Technology or Database

a) When evaluating a request for the use of surveillance technology or a database, the City Council may consider a range of factors, including but not limited to:

i) The potential public safety benefits and effectiveness of the technology.
ii) The economic, social, and community costs associated with its implementation and use.
iii) Any potential impacts on civil liberties and civil rights, including privacy concerns.
iv) The possibility of disparate impacts on specific communities or groups.
v) Safeguards or oversight mechanisms that could mitigate risks or unintended consequences.
vi) Alternative methods or technologies that could achieve similar outcomes with fewer negative effects

Section 4. Reporting and Approval of Existing Surveillance Technologies and Databases

(a) For all existing or hereinafter approved surveillance technology and databases in use, a "Surveillance Technology Annual Report" will be publicly available and presented to City

Council each year, which includes a current copy of the "Use Policy" for each technology and other information included in the definitions in Attachment A.

(b) For all surveillance technology and databases referenced here that are already in use at the time this Ordinance is approved:

(i) The City shall present to City Council a "Use Report" and "Use Policy" for each technology or database in use, within one hundred twenty (120) days of the passing of this Ordinance, unless otherwise extended with ~~written~~ approval by majority vote from City Council. No more than two (2) extensions shall be granted for any individual technology or database in use.

(ii) The existing surveillance technologies and databases shall require a formal approval process (as outlined in Section 1 and 2 of this Ordinance) as soon as the information on each technology is made available.

(iii) If the Council has not approved the continuing use of the surveillance technology, including the Use Report and the Use Policy, within one hundred eighty (180) days of its submission to the Council, unless otherwise extended, the City Department shall cease its use of the surveillance technology and the sharing of surveillance data therefrom until such time as Council approval by majority vote is obtained in accordance with this Ordinance.

(iv) During the period that continued use is not approved, the technology or database contract shall not be renewed or extended even if the result would be the termination of availability of the use before one hundred eighty (180) days.

Section 5. Contractual Agreements Involving Surveillance Technology & Databases

(a) Except where otherwise allowed under this Ordinance all contracts or agreements for the acquisition or use of surveillance technology, regardless of duration or cost, shall require formal approval by a majority vote of the City Council prior to execution.

(b) Prior to approval, the City Department shall provide all members of City Council with an unredacted copy of any and all contract(s) or other agreement(s) for the purchase, acquisition, or use of any new surveillance technology or database, including proposed non-disclosure agreements (NDAs) that are required to be executed in tandem with a purchase or acquisition agreement

(c) The Mayor's Office and all City Departments are hereby prohibited from entering into any contract or other agreement that facilitates the receipt of privately generated and owned surveillance data, or government generated and owned surveillance data, to any non-governmental entity in exchange for any monetary or any other form of consideration from any source, including the assessment of any additional fees, interest, or surcharges on unpaid fines or debts. Any contracts or agreements signed prior to the enactment of this ordinance that violate this section shall be terminated as soon as is legally permissible.

Section 6. Exigent Circumstances

(a) Notwithstanding the provisions of this ordinance, the Urbana Police Department or other City Department may temporarily acquire or temporarily use surveillance technology in exigent circumstances for a period not to exceed 30 days, with approval from the Mayor or their designee, without following the provisions of approval stated in this ordinance before that acquisition or use. No more than two (2) consecutive periods of exigent circumstantial use shall be granted for any individual technology or database.

(b) If the Urbana Police Department or other City Department acquires or uses surveillance technology in exigent circumstances under this section, the Urbana Police Department or other City Department must:

(i) Report that acquisition or use to the City Council in writing within 30 days following the end of those exigent circumstances and the use of the surveillance technology.

(ii) Submit a Use Report and, if necessary, a technology-specific Use Policy to the City Council regarding that Surveillance Technology within 30 days following the end of those Exigent Circumstances.

(iii) Include that surveillance technology in the next Surveillance Technology Annual Report to the City Council following the end of those Exigent Circumstances.

(iv) If the Urbana Police Department or other City Department is unable to meet the 30-day timeline to submit a surveillance technology Use Report and, if necessary, a technology-specific Use Policy to the City Council, the Urbana Police Department or other City Department must notify the City Council in writing requesting to extend this period. The City Council may grant extensions in 30-day increments beyond the original 30-day timeline to submit a surveillance technology Use Report, and, if necessary, a technology-specific Use Policy.

(v) Any surveillance technology Use Report, and, if necessary, any technology-specific Use Policy submitted to the City Council under this subsection shall be made publicly available on the City's website upon submission to the City Council.

(vi) Any Surveillance Technology Use Report and, if necessary, technology-specific Use Policy submitted to the City Council under this section may be redacted to the extent required to comply with an order by a court of competent jurisdiction, or to exclude information that, in the reasonable discretion of the Urbana Police Department or other City Department, would, if disclosed, materially jeopardize an ongoing investigation or otherwise represent a significant risk to public safety and security; provided, however, that any information redacted pursuant to this paragraph will be released in the next Surveillance Technology Annual Report following the point at which the reason for such redaction no longer exists.

(c) Departments using approved surveillance technologies or other technologies with unutilized and unapproved surveillance capabilities may apply a technical patch or upgrade that is necessary to mitigate cyber security threats to the City's environment. The department shall not use any unapproved new surveillance capabilities of the technology until the requirements of this ordinance are met or unless the Mayor or the Mayor's designee determines that the use is unavoidable; in that case, the Mayor shall request City Council approval as soon as possible. The request shall include a report to the City Council of how the altered surveillance capabilities were used since the time of the upgrade.

Section 7. Exclusionary Rule; Deletion/Destruction Requirement

(a) Any data or other information created or collected in contravention of this ordinance, and any data or information derived therefrom, shall be deleted and destroyed as soon as possible, in accordance with state and federal laws, and may not:

(i) Be offered as evidence by any City government entity, agency, department, prosecutorial office, or any other subdivision thereof, in any criminal or civil action or proceeding against any member of the public, except as evidence of the violation of this Act; or

(ii) Be voluntarily provided to another person or entity for use as evidence or for any other purpose.

(b) Notwithstanding the above, if, upon the discovery of data or other information that was created or collected in contravention of this ordinance, it appears such data or

information may be material to the defense in a criminal prosecution, a copy of the relevant, potentially material data or other information shall be turned over to the defendant before it is deleted and destroyed.

Section 8. Annual Surveillance Technology Report Oversight

(a) Upon request, representatives of City Council, the Civilian Police Review Board, and the Human Rights Commission shall be given full and open access to information relevant to the enforcement of this ordinance or complaints made to their Board or Commission regarding surveillance technology or databases subject to this ordinance, in compliance with the Open Meetings Act, City confidentiality policies, and other relevant state and federal laws.

(b) The Civilian Police Review Board (CPRB) shall collaborate on the Surveillance Technology Annual Report, Use Report, and Use Policy of each surveillance technology or database subject to this ordinance, with a final vote on the recommendation by CBRP before moving to the City Council, Committee of the Whole. …. (changes to CPRB ordinance)

(c) The Civilian Police Review Board and the Human Rights Commission shall hear complaints made to their Board or Commission regarding surveillance technology or databases subject to this ordinance in accordance with Chapter 19 Article 3 and Chapter 12 of the Urbana City Code of Ordinances.

From ACLU Model Bill (https://www.aclu.org/documents/community-control-over-police-surveillance-model-bill)

Section 8. Community Advisory Committee on Surveillance

(A) Within three (3) months of the adoption of this Act, the City Council shall appoint a Community Advisory Committee on Surveillance to provide the City Council with broad principles to help guide decisions about if and how surveillance technologies should be used by the City and its municipal agencies.

(1) The membership of the Community Advisory Committee on Surveillance should reflect the diversity of the City's residents, and special efforts should be made to ensure communities that have historically been disproportionately subjected to government surveillance are well-represented.

(2) The Community Advisory Committee on Surveillance shall have a Chair and Vice Chair, who shall be elected annually by the members of the Committee.

(B) Every year, by no later than September 15, the Community Advisory Committee on Surveillance shall produce and submit to the City Council a Surveillance Technology Community Equity Impact Assessment and Policy Guidance, which shall address, at a minimum, the following:

(1) What communities and groups in the City, if any, are disproportionately impacted by the use of surveillance technologies, what disparities were perceived and/or experienced, and what were the resulting adverse impacts on the community's or group's civil rights and/or civil liberties;

(2) With respect to each perceived or experienced disparity identified in response to Section 8(B)(1), what remedial adjustments to laws and policies, including but not limited to prior approvals granted pursuant to Section 1(A), should be made so as to achieve a more just and equitable outcome in the future.

(3) With respect to each remedial adjustment identified in response to Section 8(B)(2), what additional funding, implementation strategies, and/or accountability mechanisms would be needed to effectuate the adjustment; and

(4) In light of the collective responses to Section 8(B)(1)-(3), what new approaches and considerations should the City Council bring to future reviews of applications submitted pursuant to Section 1(A).

Section 9. Definitions

The list of relevant definitions is included in Attachment A as part of this Ordinance.

PASSED BY THE CITY COUNCIL this ___ day of _____, 2024.

AYES:

NAYS:

ABSTENTIONS:

Darcy E. Sanderfur, City Clerk

APPROVED BY THE MAYOR this ____ day of_____, 2024.

Diane Wolfe Marlin, Mayor

ATTACHMENT A

(Ordinance No. 2024-12-042)

Definitions:

1) Exigent Circumstances means the Urbana Police Chief or their designee's good faith and reasonable belief that an emergency involving danger of death, physical injury, or significant property damage or loss, similar to those that would render it impracticable to obtain a warrant, requires the use of the surveillance technology or the surveillance data it provides. The use of surveillance technology in exigent circumstances shall not infringe upon an individual's right to peacefully protest or exercise other lawful and protected constitutional rights. Exigent circumstances for the purposes of this temporary acquisition and use shall be of the type of emergency situations as contemplated under Chapter 6 of the City Code.

2) Surveillance means the act of observing or analyzing the movements, behavior, or actions of identifiable individuals.

3) Surveillance Data means any electronic data collected, captured, detected, recorded, retained, processed, intercepted, or analyzed by Surveillance Technology which is used or acquired by the City or operated at the direction of the City.

4) Surveillance Technology means any device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, associational, or similar information specifically associated with, or capable of being associated with, any identifiable individual or group; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software.

a) Examples of Surveillance Technology include, but are not limited to:

1. International mobile subscriber identity (IMSI) catchers and other cell-site simulators;
2. Automatic license plate readers;
3. Electronic toll readers;
4. Closed-circuit television cameras except as otherwise provided herein;
5. Biometric Surveillance Technology, including facial, voice, iris, and gait-recognition software and databases;
6. Mobile DNA capture technology;
7. Gunshot detection and location hardware and services;
8. GPS tracking systems that monitor an individual's location without authorization;
9. X-ray vans;

10. Video and audio monitoring and/or recording technology, such as surveillance cameras;
11. Surveillance enabled or capable light bulbs or light fixtures;
12. Tools, including software and hardware, used to gain ~~unauthorized~~ access to a mobile device, computer, computer service, or computer network;
13. Social media monitoring software;
14. Through-the-wall radar or similar imaging technology;
15. Passive scanners of radio networks;
16. Long-range Bluetooth and other wireless-scanning devices;
17. Thermal imaging or "forward-looking infrared" devices or cameras;
18. Electronic database systems containing Surveillance Data about Identifiable Individuals;
19. Radio-frequency identification (RFID) scanners; and
20. Software designed to integrate or analyze data from surveillance technology, including surveillance target tracking and predictive policing software.

b) Surveillance Technology does not include the following devices, software, or hardware, which are exempt from the requirements of this ordinance, unless the devices, hardware, or software are modified to include additional surveillance capabilities:

1. Routine office hardware, such as televisions, computers, and printers, that are in widespread public use and will not be used for any surveillance or surveillance- related functions;
2. Parking ticket devices (PTDs) and related databases;
3. Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is used for manually capturing and manually downloading video and/or audio recordings;
4. Cameras installed in or on a police vehicle;

#. Body-worn cameras as required by the Illinois Law Enforcement-Worn Body Camera Act, 50 ILCS 706/10-1 *et seq.*, as amended;

5. Cameras installed pursuant to state law authorization in or on any vehicle or along a public right-of-way solely to record traffic violations or traffic patterns, provided that the Surveillance Data gathered is used only for that purpose;
6. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
7. City databases that do not and will not contain any Surveillance Data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by Surveillance Technology;

8. Manually-operated technological devices that are used primarily for internal City communications and are not designed to surreptitiously collect Surveillance Data, such as radios and email systems;
9. Parking access and revenue control systems, including proximity card readers and transponder readers at City-owned or controlled parking garages;
10. Card readers and key fobs used by City employees and other authorized persons for access to City-owned or controlled buildings and property;
11. Cameras installed on City property solely for security purposes, including closed-circuit television cameras installed by the City to monitor entryways and outdoor areas of City-owned or controlled buildings and property for the purpose of controlling access, maintaining the safety of City employees and visitors to City buildings, and protecting City property;
12. Security cameras including closed-circuit television cameras installed by the City to monitor cashiers' windows and other cash-handling operations and to maintain the safety of City employees and visitors to such areas;
13. Cameras installed solely to protect the physical integrity of City infrastructure; and
14. Technology that monitors only City employees in response to complaints of wrongdoing or in order to prevent waste, fraud, or abuse of City resources.

(c) "Use Report" shall mean a publicly released, legally enforceable written report that includes, at a minimum, the following:

(i) Information describing the surveillance technology and how it works;

(ii) Information on the proposed purpose(s) of the surveillance technology;

(iii) If the surveillance technology will not be uniformly deployed throughout the city, what factors will be used to determine where the technology will be deployed or targeted;

(iv) The fiscal impact of the surveillance technology;

(v) An assessment of whether use of the surveillance technology will have an unwarranted disparate impact on protected classes and demographics, as defined in the Illinois Civil Rights Act of 2003, the Urbana Human Rights Ordinance, and other relevant laws and policies.

(vi) An assessment identifying any potential adverse impacts the surveillance technology, if deployed, might have on civil liberties and civil rights, and what specific, affirmative measures will be implemented to safeguard the public from the potential adverse impacts.

(d) "Use Policy" shall mean a publicly released, legally enforceable written policy governing the use of the surveillance technology that, at a minimum, includes and addresses the following:

(i) What specific purpose(s) the surveillance technology is intended to advance.

(ii) Description of the authorization for use of the policing technology: specifically, what legal and procedural rules will govern each authorized use; what potential uses of the surveillance technology will be expressly prohibited such as the warrantless surveillance of public events and gatherings; and how and under what circumstances will surveillance data that was collected, captured, recorded, or intercepted by the police technology be analyzed and reviewed.

(iii) Description of data collection, protection, and retention: specifically, what types of surveillance data will be collected, captured, recorded, intercepted, or retained by the police technology; what safeguards will be used to protect surveillance data from unauthorized access; for what maximum limited time period the surveillance data will be retained; and by what process the surveillance data will be regularly deleted after the retention period.

(iv) Description of data sharing: specifically, which governmental agencies, departments, bureaus, divisions, or units will be approved for data sharing; how such sharing is necessary for the stated purpose and use of the surveillance technology; and what mechanisms will ensure any entity sharing access to the surveillance technology or surveillance data complies with the applicable surveillance use requirements within the Urbana "Use Policy" and does not further disclose the surveillance data to unauthorized persons and entities.

(e) "Surveillance Technology Annual Report" shall mean a written report covering each surveillance technology in use over the past year that is publicly released at least once per year and shall, at a minimum, include the following:

(i) A summary of how each surveillance technology and database was used.

(iii) Total annual costs for each surveillance technology and database, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.

(iii) How often collected surveillance data was shared with and received from any external persons or entities; under what legal standard(s) the information was disclosed; and the justification for the disclosure(s).

(iv) A summary of complaints or concerns that were received about each surveillance technology and database.

(v) The results of any internal audits, any information about violations of the Use Policy, and any actions taken in response to complaints or concerns.

(vi) Justification for the continued use of each surveillance technology and database and safeguards to protect civil liberties, privacy, and against discrimination.