

**DATE:** Monday, December 15, 2025  
**TIME:** 7:00 PM  
**PLACE:** 400 South Vine Street, Urbana, IL 61801

---

## AGENDA

*Chair: Jaya Kolisetty, Ward 4*

- A. Call to Order and Roll Call
- B. Approval of Minutes of Previous Meeting
- C. Additions to the Agenda
- D. Presentations and Public Input
- E. Staff Report
- F. New Business
  - 1. **Resolution No. 2025-12-094R:** A Resolution Approving an Increase in the Number of Liquor License in the Class INC Designation for Champaign-Urbana Adventures in Time and Space, LLC, d/b/a Parcadia, 302 North Broadway Avenue, Suite 100, Urbana, Ill. – Exec
- G. Discussion
  - 1. **Police Surveillance Technology Continuing Discussion (Ordinance No. 2024-12-042)**
- H. Council Input and Communications
- I. Adjournment

## 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](mailto: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@urbanil.gov](mailto:CityClerk@urbanil.gov)

**RESOLUTION NO. \_\_\_\_\_**

**A RESOLUTION APPROVING AN INCREASE IN THE NUMBER OF LIQUOR LICENSES IN THE CLASS INC DESIGNATION FOR CHAMPAIGN-URBANA ADVENTURES IN TIME AND SPACE, LLC, D/B/A PARCADIA, 302 NORTH BROADWAY AVENUE, SUITE 100, URBANA, ILL.**

**WHEREAS**, the City Council has adopted Urbana City Code Section 3-42 to establish limits on the number of liquor licenses issued in the City; and

**WHEREAS**, Section 3-42(c) of the Urbana City Code provides that a majority of the corporate authorities then elected to office have to approve the creation of a new license; and

**WHEREAS**, an application for a liquor license in the Class INC designation has been submitted to the Local Liquor Commissioner; and

**WHEREAS**, the City Council finds that the best interests of the City are served by increasing the number of liquor licenses in the Class INC designation by one for Champaign-Urbana Adventures in Time and Space, LLC, d/b/a Parcadia, 302 North Broadway Avenue, Suite 100, Urbana, Ill.

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

The maximum number of liquor licenses in the Class INC designation is hereby increased by one for Champaign-Urbana Adventures in Time and Space, LLC, d/b/a Parcadia, 302 North Broadway Avenue, Suite 100, Urbana, Ill. The schedule of maximum number of authorized licenses for the respective classification maintained by the Local Commissioner shall reflect such increase.

**PASSED BY THE CITY COUNCIL** this Date day of Month, Year.

AYES:

NAYS:

ABSTENTIONS:

\_\_\_\_\_  
Darcy E. Sandefur, City Clerk

**APPROVED BY THE MAYOR** this Date day of Month, Year.

\_\_\_\_\_  
DeShawn B. Williams, Mayor

**Examples of Covered/ included Surveillance Technology (not an exhaustive list)**

<b>Urbana, IL</b>	<b>Oak Park, IL</b>	<b>Boston, MA</b>	<b>Oakland, CA</b>	<b>Dayton, OH</b>
Automatic license plate readers;	✓	✓	✓	✓
International mobile subscriber identity (IMSI) catchers and other cell-site simulators	✓ (Cell site simulators, stingrays)	✓	✓	✓
Biometric Surveillance Technology, including facial, voice, iris, and gait-	✓ (face & gait only)	✓	✓	✓ (face & gait only)
Social media monitoring software	✓	✓	✓	✓
Video and audio monitoring and/or recording technology <u>that can be remotely accessed, including privately owned devices such as doorbell cameras</u>	✓(all cameras with remote access	✓	✓(all cameras with remote access	✓(all cameras with remote access
Closed-circuit television cameras except as otherwise provided herein	✓(all cameras with remote access	✓	✓(all cameras with remote access	✓(all cameras with remote access
Gunshot detection and location hardware and services	✓	✓	✓	✓
Software designed to integrate or analyze data from surveillance technology,	✓	✓	✓ (similar)	✓
Thermal imaging or “forward-looking infrared” devices or cameras	✓ in definition	✓	✓	✓ in definition
Surveillance enabled or capable light bulbs or light fixtures	✓	✓		✓
GPS tracking systems that monitor an individual’s location, <u>in accordance with the IL Freedom from Location Surveillance Act.</u>	✓ "location info" in definition			✓ "location info" in definition
Electronic database systems containing <u>or analyzing</u> Surveillance Data about	✓ in definition	✓	✓ in definition	✓ in definition
Tools, including software and hardware, used to gain unauthorized access to a mobile device, computer, computer service, or computer network	✓ vaguely in definition	✓	✓ vaguely in definition	✓ vaguely in definition
<u>Drone usage in City limits. in addition to compliance with the Illinois Freedom.</u>	✓ cites IL drone surv act			
Through-the-wall radar or similar imaging technology		✓		
X-ray vans		✓		
Radio-frequency identification (RFID) scanners		✓		
Passive scanners of radio networks		✓		
Long-range Bluetooth and other wireless-scanning devices		✓		
Electronic toll readers;		✓		
Mobile DNA capture technology		✓		
			Body-worn cameras	

<b>General Definition of Surveillance Technology</b>					Applies to:
<b>Urbana</b>	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.				TBD
<b>Oak Park, IL</b>	Any device or system designed, used, or intended to be used to collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory, or similar information associated with, or capable of being associated with, any specific individual or group of specific individuals by the Police Department for law enforcement purposes.				Police Department
<b>Boston, MA</b>	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.				All city departments, mayor submits to council
<b>Oakland, CA</b>	Any software, electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group.				All city staff
<b>Dayton, OH</b>	Any device or system designed or used or intended to be used to collect, retain, process or share audio, electronic, visual, location, thermal, olfactory, or similar information associated with, or capable of being associated with, any specific individual or group of specific individuals by the Dayton Police Department.				Police Department
<b>NOT covered by the ordinance/ code as surveillance tech</b>					
	<b>Urbana, IL</b>	<b>Oak Park, IL</b>	<b>Boston, MA</b>	<b>Oakland, CA</b>	<b>Dayton, OH</b>
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	✓		✓	✓	✓
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	✓		✓	✓	✓
Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles	✓		✓	✓	✓
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	✓ (similar)		✓	✓ (including payroll, accounting, fiscal data)	✓ (including payroll, accounting, fiscal data)

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	✓	✓	✓	✓
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	✓ (similar)	✓		✓ (similar)
Technology that monitors only City employees in response to complaints of wrongdoing or in order to prevent waste, fraud, or abuse of City resources	✓ (similar)	✓		✓ (similar)
Parking ticket devices (PTDs) and related databases	✓	✓		✓
Card readers and key fobs used by City employees and other authorized persons for access to City-owned or controlled buildings and property	✓ (similar)	✓		
Cameras installed in or on a police vehicle	✓	✓		
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	✓ (similar)	✓		
Parking access and revenue control systems, including proximity card readers and transponder readers at City-owned or controlled parking garages	✓ (similar)	✓		
Body-worn cameras as required by the Illinois Law Enforcement-Worn Body Camera Act, 50 ILCS 706/10-1 <i>et seq.</i> , as amended	✓			
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;		✓		✓ (similar)
Cameras installed solely to protect the physical integrity of City infrastructure		✓		

		Police Department computer aided dispatch (CAD), records/case management, live scan, booking, and related dispatch and operation or emergency services systems and state and federal law enforcement databases;		✓ Police department case management and records management systems, including computer aided dispatch systems, and field-based reporting systems.	✓
		Police department interview room, holding cell, and Police Department internal security audio/video recording systems;		✓ (interview room cameras only)	✓
		Smart meter technology employed for water and sewer utility purposes			
				Personal communication devices that have not been modified beyond stock manufacturer capabilities in a manner described above, provided that any bundled Face Recognition Technology is only used for the sole purpose of user authentication in the regular course of conducting City business.	

Ordinance No. 2024-12-042

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

**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 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 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 the data it collects by the City of Urbana police department, and to protect privacy, civil rights, and racial and immigrant justice.

## **Section 2. Approval Process for Surveillance Technology Acquisition or Use**

(a) When the Police Department seeks to acquire or use new surveillance technology or change an existing Use Policy, it shall, prior to such acquisition or use obtain approval by majority vote of the Urbana City Council prior to purchasing, acquiring, or using any new surveillance technology (as defined in Attachment A of this Ordinance), which includes adding data from a new source or new analytic tools in a manner which changes the functionality of the existing data collected by the surveillance technology.

(b) At least thirty (30) days prior to seeking approval of a surveillance technology, the City shall submit to the City Council and make publicly available a written and unredacted surveillance technology “Use Report,” along with a draft of the proposed surveillance technology “Use Policy” (*as defined in Attachment A of this Ordinance*). During this time, the public will have the opportunity to provide input to the City Council.

## **Section 3. Standard for Approval of Surveillance Technology**

a) When evaluating a request for the use of surveillance technology, 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**

(a) For all existing or hereinafter approved surveillance technology 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 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 in use, within one hundred twenty (120) days of the passing of this Ordinance, unless otherwise extended with 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 shall require a formal approval process (as outlined in Section 2 and 3 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 yet 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.
- (c) Any two council members may request that a surveillance technology be re-evaluated for approval as outlined in Section 2 and 3 of this Ordinance.

### **Section 5. Contractual Agreements Involving Surveillance Technology**

- (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 shall provide all members of City Council with a complete copy of any and all contract(s) or other agreement(s) for the purchase, acquisition, or use of any new surveillance technology, 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 with 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), that facilitates the receipt of government or privately generated and owned surveillance data. 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 may temporarily acquire or temporarily use surveillance technology in exigent circumstances for a period not to exceed thirty (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 acquires or uses surveillance technology in exigent circumstances under this section, the Department must:

(i) Report that acquisition or use to the City Council in writing within thirty (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 thirty (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 maintain essential operations or 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 collected by surveillance technology 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 voluntarily 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) The Civilian Police Review Board (CPRB) shall review each Surveillance Technology Annual Report, Use Report, and Use Policy of surveillance technology or database subject to this ordinance, with a final vote on the recommendation by CBRP before moving to the Urbana City Council Committee of the Whole. If the CPRB is not able to review the reports and policies in a reasonable time-frame due to logistical factors, the City Department will present the reason for lack of CPRB review to council.
  
- (b) 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.
  
- (c) 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.

**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* mean occurrences that are determined by the Mayor or their designee to meet the definition of a “disaster” under the Illinois Emergency Management Agency Act (220 ILCS 3305/1 et seq), meaning “an occurrence or threat of widespread or severe damage, injury or loss of life or property resulting from any natural, technological, or human cause, including but not limited to fire, flood, earthquake, wind, storm, hazardous materials spill or other water contamination requiring emergency action to avert danger or damage, epidemic, air contamination, blight, extended periods of severe and inclement weather, drought, infestation, critical shortages of essential fuels and energy, explosion, riot, hostile military or paramilitary action, public health emergencies, cyber incidents, or acts of domestic terrorism.” 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.
  
- 2) *Surveillance* means the act of observing or analyzing the movements, behavior, or actions of identifiable individuals.
  
- 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 monitoring device, hardware, or software.

### Reconsider definitions, compare with other places, consider private cameras

- 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 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
- #. Drone usage in City limits, in addition to compliance with the Illinois Freedom from Drone Surveillance Act
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, and the location(s) where it may be deployed and crime statistics for such location(s).
- (iv) The fiscal impact of the surveillance technology, including initial purchase and other known ongoing costs, including impact on personnel time, along with any current or potential sources of funding.
- (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.

(vii) Whether use or maintenance of the surveillance technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis.

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

(ii) Description of the authorization for use of the surveillance 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.

(v) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

(vi) Auditing and Oversight: The mechanisms to ensure that the surveillance use policy is followed, including internal personnel assigned to ensure compliance with the surveillance use policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority.

(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 was used, including locations and neighborhoods where technology or equipment was deployed, and information that may assist the City Council to assess whether the surveillance technology has been effective at achieving its identified purposes.
- (ii) 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 and what type of 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.
- (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.

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 Definition 1, 4.a.8, which describes GPS data collection <i>without authorization</i> .
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 interested 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 Environmental 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	IDCore	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.