Non-Regulatory Guidance to Law Enforcement Agencies:
Drone Usage

I. Introduction

Illinois law regulating drone usage by state and local law enforcement agencies[1] has changed. In June 2023, the Drones as First Responders Act became law, amending the Freedom from Drone Surveillance Act.[2] As discussed in more detail in this guidance, the Act's requirements governing drone usage by law enforcement include:

- Law enforcement agencies generally may not use drones to gather information, except in certain circumstances specified by the Act.[3]
    - Some of the Act's exceptions include when the agency obtains a search warrant, when engaged in a search-and-rescue operation (and not a criminal investigation), and in certain limited ways during a routed or special event like a parade or food festival.[4]
    - Information collected by drones under the Act's exceptions must be retained and destroyed within certain timetables specified in the Act.[5]
- Law enforcement agencies are strictly prohibited from using drones in certain specific ways, even when the drone usage would otherwise be allowed by the Act.
    - For example, law enforcement agencies must not use drones solely to surveil activities protected by the First Amendment, must not use drones to conduct warrantless searches in contravention of the Fourth Amendment, and must not equip drones with lethal or non-lethal weapons.[6]

[1] The Act defines law enforcement agency as "any agency of this State or a political subdivision of this State which is vested by law with the duty to maintain public order and to enforce the criminal laws." 725 ILCS 167/5.
[2] The current law, including all amendments, is codified as 725 ILCS 167/1 to 725 ILCS 167/45 (the "Act").
[3] *See* 725 ILCS 167/10 (exceptions listed at 725 ILCS 167/15).
[4] *See* 725 ILCS 167/15(2); /15(4); /15(10).
[5] 725 ILCS 167/20.
[6] *See* 725 ILCS 167/15(2); /15(10); /18.

- Any law enforcement agency that uses a drone must implement a policy governing the operation, use, administration, and oversight of its drone program, and must make that policy publicly available on its website.[7]

- Any law enforcement agency that owns one or more drones must provide an annual report in writing to the Illinois Criminal Justice Information Authority (ICJIA), including a copy of its drone policy and data on the number of drones, drone flights, and drone usage by the agency per the Act's specifications.[8]

The Act grants the Office of the Illinois Attorney General ("OAG") authority to investigate potential patterns or practices of violations of the Act. OAG issues this non-regulatory guidance to Illinois law enforcement agencies and Illinois residents to provide additional information regarding compliance with the Act's requirements and best practices.

II. When can law enforcement agencies use drones?

The Act broadly prohibits a state or local law enforcement agency from using a drone to gather information, except in certain specified circumstances.[9] The Act defines "information" as "any evidence, images, sounds, data, or other information gathered by a drone."[10] Examples of information-gathering by drones might include taking photographs, recording video, collecting biometrics including body temperatures through thermal detection, or live-streaming video footage from the drone to a member of the law enforcement agency. Information collected in violation of the Act's limitations "shall be presumed to be inadmissible in any judicial or administrative proceeding."[11]

There are ten narrow exceptions to the Act's broad restriction. Accordingly, Illinois law enforcement agencies may use a drone *only* when the use is expressly authorized by one of the following exceptions:

a. Terrorist Attack Exception (725 ILCS 167/15(1))

An agency may use a drone to counter a high risk of a terrorist attack by a specific individual or organization. This "high risk" requirement may only be satisfied where "the United States Secretary of Homeland Security determines that credible intelligence indicates that there is that risk."

b. Search Warrant Exception (725 ILCS 167/15(2))

An agency may use a drone if it obtains a search warrant issued under Section 108-3 of the Code of Criminal Procedure. The warrant must be limited to a period of 45 days, renewable by a judge upon a showing of good cause for subsequent periods of 45 days.

---

[7] *See* 725 ILCS 167/35(c).
[8] *See* 725 ILCS 167/35(a).
[9] *See* 725 ILCS 167/10 (exceptions listed at 725 ILCS 167/15).
[10] 725 ILCS 167/5.
[11] 725 ILCS 167/30.

c. Imminent Harm to Life, Imminent Escape and Evidence Destruction Exception (725 ILCS 167/15(3))

An agency may use a drone if it has reasonable suspicion that swift action is needed to prevent: (1) imminent harm to life, (2) the imminent escape of a suspect, or (3) the destruction of evidence. Use under this exception is limited to a period of 48 hours.

Where this exception is invoked, the chief executive officer of the agency must report the use in writing to the local State's Attorney within 24 hours of the *initiation* of this use.

d. Missing Person and Search and Rescue (725 ILCS 167/15(4))

An agency may use a drone to locate a missing person, engage in a search and rescue operation, or aid a person who cannot otherwise be safely reached, as long as the agency is not using the drone to conduct a criminal investigation.

e. Crime and Crash Scene (725 ILCS 167/15(5))

An agency may use a drone to take photographs of crime scenes and traffic crash scenes, but this use must be conducted in a geographically confined and time-limited manner to document specific occurrences. Agencies must make every reasonable attempt to photograph only the crime scene or traffic crash scene and avoid other areas. Once an agency has obtained photographs of the crime scene or traffic crash scene, the agency should promptly conclude its drone use in that area.

This exception does not allow taking photographs of private property, unless the law enforcement agency has either a search warrant or lawful consent to search.[12]

f. Disaster and Public Health Emergency (725 ILCS 167/15(6))

An agency may use a drone to collect information during a disaster or public health emergency, as defined by Section 4 of the Illinois Emergency Management Agency Act.[13] An

---

[12] No search warrant or consent to search is required for use of a drone under this exception on lands, highways, roadways, or areas belonging to this State or a political subdivision of this State. 725 ILCS 167/15(5).

[13] The Illinois Emergency Management Agency Act defines "disaster" as "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." 20 ILCS 3305/4. The Act defines "public health emergency" as "an occurrence or imminent threat of an illness or health condition that: (a) is believed to be caused by any of the following: (i) bioterrorism; (ii) the appearance of a novel or previously controlled or eradicated infectious agent or biological toxin; (iii) a natural disaster; (iv) a chemical attack or accidental release; or (v) a nuclear attack or accident; and (b) poses a high probability of any of the following harms: (i) a large number of deaths in the affected population; (ii) a large number of serious or long-term disabilities

official declaration of a disaster or public health emergency is not necessary for this exception to apply. For example, a drone may be used to obtain information necessary to determine whether to declare a disaster or public health emergency, monitor weather or emergency conditions, survey damage, or otherwise coordinate response and recovery efforts. The exception permits use during the disaster or public health emergency and during response and recovery efforts.

g. Infrastructure Inspection (725 ILCS 167/15(7))

If a local government agency expressly asks law enforcement to inspect the infrastructure of a building or other structure, the law enforcement agency may use a drone to collect information as part of that requested infrastructure inspection. The law enforcement agency must make every reasonable attempt to photograph only the identified building or structure and to avoid other areas. The law enforcement agency must turn over all information gathered to the requesting local government agency as soon as practicable, and immediately destroy any copies in its possession.

h. Public Relations Demonstration (725 ILCS 167/15(8))

An agency may use a drone to demonstrate the capabilities and functionality of the police drone for public relations purposes, provided no information is collected or recorded by the drone during the demonstration.

i. Public Safety Answering Point Calls (725 ILCS 167/15(9))

An agency may use a drone for three specific purposes in response to a Public Safety Answering Point (or 911) call for service.[14] The only three purposes for which a drone is allowed to be used under this exception are: (1) for one or more responders to locate victims, (2) to assist with immediate victim health or safety needs, or (3) to coordinate the response of emergency vehicles and personnel to an emergency.

j. Routed or special events (725 ILCS 167/15(10))

An agency may use a drone at a routed event or special event, such as a parade or community festival. However, political protests, marches, demonstrations, or other assemblies protected by the First Amendment are not routed events or special events under the Act and do not fall under this exception. A law enforcement agency generally may not use drones at those assemblies.

Law enforcement drone usage at a routed or special event is subject to several restrictions under the Act. Agencies may only use a drone pursuant to this exception if:

---

in the affected population; or (iii) widespread exposure to an infectious or toxic agent that poses a significant risk of substantial future harm to a large number of people in the affected population." 20 ILCS 3305/4.

[14] Public Safety Answering Points are defined as the "primary answering location of an emergency call that meets the appropriate standards of service and is responsible for receiving and processing those calls and events according to a specified operational policy." Emergency Telephone System Act, 50 ILCS 750/2.

- The event is a parade, walk, or race (a routed event) or a concert or food festival (a special event) that:

  (1) is hosted by the State, a county, a municipality, a township, or a park district,

  (2) is outdoors and open to the public, and

  (3) meets the Act's specific attendance requirements. Routed events must have an estimated attendance of more than 50 people while special events must have an estimated attendance of 150 to 500 people, depending on the population of the unit of local government hosting the event.

- Notice of the drone usage must be posted at the event location including at major entry points for at least 24 hours before the event. The notice must clearly communicate that drones may be used at the upcoming event for the purpose of real-time monitoring of participant safety.

- Drones may be used *prior* to the event, before participants have begun to assemble, only to create maps and determine appropriate access routes, staging areas, and traffic routes. During drone usage before the event, no personal identifying information may be recorded, and no recorded information may be used in any criminal prosecution.

- Drones may be used *during* the event only to:

  (1) Detect a breach of event space, including a breach by an unauthorized vehicle, an interruption of the parade route, or a breach of an event barricade or fencing;

  (2) Evaluate crowd size and density;

  (3) Identify activity that could create a public safety issue for the crowd as a whole, such as crowd movement;

  (4) Assist in the response of personnel to a public safety incident; or

  (5) Assess traffic and pedestrian flow around the event.

- The drone must be flown in accord with Federal Aviation Administration safety regulations.[15]

[15] *See generally*, Federal Aviation Administration, *Public Safety and Law Enforcement Toolkit,* available at https://www.faa.gov/uas/public_safety_gov/public_safety_toolkit.

The Act specifies that law enforcement cannot use drones under this exception to surveil events or assemblies protected by the First Amendment.[16] This restriction applies regardless of location, size, particular cause, or permit status of the First Amendment protected event or assembly. Some examples of events or assemblies at which law enforcement may not use drones to gather information on individuals exercising their First Amendment rights include:

- A permitted rally at a public forum, such as a city plaza
- An unpermitted sidewalk protest targeting a government facility
- A protest march along public streets (whether permitted or unpermitted)
- An unpermitted demonstration by protestors at a routed or special event.[17]

Where an event includes both a drone use permitted under this exception as well as First Amendment protected activity, such as a political or protest group marching in an Independence Day parade, law enforcement may not use the drone to gather information on the First Amendment protected assembly (such as gathering information on protesters' identities) but may use the drone for the Act's specified purposes at the routed or special event (such as monitoring traffic flow around a parade). Law enforcement agencies are encouraged to be sensitive to the potential chilling effect that drone presence may have on First Amendment protected activity.

III. What absolute restrictions does Illinois law place on law enforcement drone use?

Even if a particular drone flight is otherwise permissible under one of the Section 15 exceptions, the following strict prohibitions apply:

a. No Warrantless Searches in Violation of the Fourth Amendment

Drones may not be used to conduct warrantless searches in contravention of the Fourth Amendment. The Fourth Amendment of the United States Constitution prohibits unreasonable search and seizure. A search occurs "when an expectation of privacy that society is prepared to consider reasonable is infringed." *United States v. Karo*, 468 U.S. 705, 712 (1984). For example, law enforcement may infringe a homeowner's reasonable expectation of privacy by using thermal imaging on a drone to measure heat emanating from inside a home. *Kyllo v. United States*, 533 U.S. 27 (2001). Accordingly, law enforcement must first obtain a search warrant before using a drone to collect information from a space in which people have a reasonable expectation of privacy. Any use of a drone pursuant to a search warrant shall be limited to a period of 45 days.[18] Information collected by use of a drone pursuant to a search warrant shall be destroyed within 30 days after being gathered.

[16] 725 ILCS 167/5, 167/15(10).
[17] The definitions for parade and routed or special event under the statute expressly exclude any political protest, march, demonstration, or other assembly protected by the First Amendment. 725 ILCS 167/5.
[18] 725 ILCS 167/15(2).

b. Limits on Use of Facial Recognition Software

A law enforcement agency operating a drone "is prohibited from using, during a flight, onboard facial recognition software that works in conjunction with the drone."[19]

A law enforcement agency may not use any information gathered by a drone with facial recognition software, unless either "(i) the law enforcement agency is using a drone to counter a high risk of a terrorist attack by a specific individual or organization and the United States Secretary of Homeland Security has determined that credible intelligence indicates that there is such a risk, or (ii) the law enforcement agency possesses reasonable suspicion that, under particular circumstances, swift action is needed to prevent imminent harm to life or to forestall the imminent escape of a suspect or the destruction of evidence."[20]

c. No Lethal or Non-Lethal Weapons

Drones may not be equipped with or use a firearm, weaponized laser, kinetic impact projectile, chemical agent or irritant, or any other lethal or non-lethal weapon.[21]

d. Limits on Information Gathered by Drones Owned by Private Third Parties

An agency generally may not acquire information from a drone owned by a private third party or direct the acquisition of information through the use of a drone owned by a private third party.[22] This restriction does not, however, prevent a private third party from voluntarily submitting information acquired by a privately owned drone to law enforcement.

A law enforcement agency must comply with the strict information retention and destruction requirements of the Act (see Section VI, below) if it acquires information from a privately owned drone, such as when a private third party voluntarily submits such information on their own initiative.

IV. What steps must law enforcement take before implementing a drone program?

Each law enforcement agency that uses a drone must implement and make publicly available on its website the agency's policy governing the operation, use, administration, and oversight of its drone program.[23] The policy must outline the program's drone use consistent with the requirements of the Act[24] and federal law.[25] The policy also must include a provision requiring

---

[19] 725 ILCS 167/17.
[20] *Id*.
[21] 725 ILCS 167/18.
[22] 725 ILCS 167/40. The Act states that an exception to this restriction may be made as provided under Section 15, but Section 15 does not specify any exceptions to permit the acquisition of information through a drone owned by a private third party.
[23] 725 ILCS 167/35(c).
[24] 725 ILCS 167/45(a).
[25] *See generally*, Federal Aviation Administration, *Public Safety and Law Enforcement Toolkit,* available at https://www.faa.gov/uas/public_safety_gov/public_safety_toolkit.

the agency to immediately take action to prevent future violations of the Act once it learns of a violation. This includes stating the means the agency will take to prevent repeated violations of the Act, such as training, discipline (including progressive discipline for repeat violations), and/or other means.[26]

Additionally, if an agency learns of willful and wanton violations of the Act, the agency must immediately remove the pilot in question from the drone program and take further action to prevent future willful and wanton violations of the Act.[27] Willful and wanton violations include instances where a drone pilot knows, or recklessly disregards, the fact that he or she is violating the Act.

OAG recommends that law enforcement agencies' required drone policies comport with the following best practices: [28]

- State the purpose of the agency's drone program and list the specific Section 15 exceptions under which the agency intends to use drones;
- Include all relevant restrictions placed on drone usage by the Act and other sources of law, including Federal Aviation Administration rules (including specific language stating law enforcement cannot use drones under Section 15(10) to surveil events or assemblies protected by the First Amendment);
- Describe the staffing requirements for the agency's drone program, including a description of each program-specific position and the responsibilities and duties particular to that position;
- Explain all training requirements for drone team pilots or other staff;
- List all standard operating procedures required from start to finish of each drone mission, including any pre-flight notice requirements and post-flight reporting and data destruction required by the Act.

[26] This provision is required under 725 ILCS 167/45(a).
[27] 725 ILCS 167/45(a).
[28] Agencies crafting drone program policies are encouraged to consult Chapter 2 of the Police Executive Research Forum. 2020. *Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks.* Washington, DC: Office of Community Oriented Policing Services, available at https://portal.cops.usdoj.gov/resourcecenter/content.ashx/cops-w0894-pub.pdf. This chapter includes sample policy language for law enforcement agencies to consider.

V. What data must be reported to the Illinois Criminal Justice Information Authority?

Law enforcement agencies that own one or more drones must provide an annual report in writing to the Illinois Criminal Justice Information Authority (ICJIA) by April 1 of each year.[29] The annual report must contain the following information: [30]

- A copy of the agency's policy regarding its drone program;
- The number of drones the agency owns;
- The number of times a drone was used pursuant to each Section 15 exception; and
- For each drone flight: when the flight occurred, why the agency used a drone, what information the agency collected, location, whether video was recorded, and whether the video is designated for retention for training purposes.

The Act also requires ICJIA to publish an annual report on its website, by July 1 of each year, listing every law enforcement agency that owns a drone, the above data for each drone usage, and a copy of the agency's latest policy concerning drones.[31]

VI. What requirements govern disclosure and retention of information collected by drones?

The Act contains different information retention and destruction requirements depending on which Section 15 exception applies to the drone usage:

Applicable Section 15 Exception	**Retention Requirement[32]**
Terrorist Attack	Must destroy information collected within 30 days of collection
Search Warrant Exception	Must destroy information collected within 30 days of collection
Imminent harm to life, imminent escape, and evidence destruction	Must destroy information collected within 30 days of collection
Missing person and search and rescue	Must destroy information collected within 30 days of collection

[29] 725 ILCS 167/35(a).
[30] *Id*.
[31] 725 ILCS 167/35(b). *See* https://icjia.illinois.gov/innovation-and-digital-services/drone/ for reports.
[32] The Act's information retention requirements are set out in 725 ILCS 167/20.

Applicable Section 15 Exception	Retention Requirement[32]
Crime and crash scene photography	Must destroy information collected within 30 days of collection
Disaster and public health emergency	Must destroy information collected within 30 days of collection
Infrastructure inspection	Must turn over information collected to the requesting local government agency as soon as practicable; all information collected must be destroyed immediately after being turned over to local government agency
Public relations	**No information may be collected**
Public Safety Answering Point calls	Must destroy information collected within 30 days of collection
Routed or special events	Must destroy information collected within **24 hours** of collection

A supervisor at the agency may retain particular information if:[33]

(1) There is reasonable suspicion that it contains evidence of criminal activity;

(2) It is relevant to an ongoing investigation or pending criminal trial;[34]

(3) It will be used exclusively for training purposes, provided that it does not contain any personally identifiable information; or

(4) It is only flight path data, metadata, or telemetry information of the drone.

Law enforcement records of drone use, including flight path data, metadata, or telemetry information of specific flights, if available, are expressly subject to the Illinois Freedom of Information Act.[35]

[33] 725 ILCS 167/20(b).

[34] Agencies conducting investigations that include information collected by drone must be mindful of their obligation to retain and disclose evidence favorable to the accused, imposed by *Brady* and its progeny. *See Brady v. Maryland*, 373 U.S. 83, 87 (1963) ("[T]he suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.").

[35] 725 ILCS 167/25(b).

The Act prohibits the disclosure or sale of any information collected during drone use to any person to whom disclosure is not authorized.[36] However, the Act expressly provides that an agency may disclose information to another governmental agency if (1) there is reasonable suspicion that the information contains evidence of criminal activity or (2) the information is relevant to an ongoing investigation or pending criminal trial.[37] When responding to requests for information disclosure to another government agency, Illinois law enforcement must be mindful that the Illinois TRUST Act generally prohibits Illinois law enforcement from sharing information with federal immigration agents, with limited exceptions.[38] Furthermore, nothing in the Act prevents disclosure of information through a court order or subpoena in connection with a criminal proceeding or if the disclosure is in regard to a completed traffic crash investigation.[39]

VII. What best practices should law enforcement agencies implement?

Law enforcement agencies should consider the following best practices[40] when implementing a drone program:

- **Establish transparency with community members.** Drone technology is both relatively new and quickly evolving. An agency should publicly announce its intent to implement a drone program and provide avenues for feedback and open communication with community members regarding the agency's plans and policies. Agencies should aim to understand and address potential concerns regarding drone use, including concerns regarding privacy and other civil liberties.[41]

- **Establish clear goals.** Prior to purchasing equipment and staffing an agency drone team, an agency should determine how it will use the drone. Agencies should closely review the Act to confirm that any intended uses fall within one of the exceptions in Section 15 of the Act. Identifying and communicating these goals will benefit community members and will also allow an agency to accurately estimate the drone program's costs.

- **Consult federal, state, and local law prior to implementation.** Agencies should consult Federal Aviation Administration regulations to ensure the

[36] 725 ILCS 167/25(c).
[37] 725 ILCS 167/25(a).
[38] See, generally, Illinois Attorney General Raoul, *Guidance: Illinois Laws Governing Law Enforcement Interactions with Immigrant Communities* (last updated 2025), available at https://illinoisattorneygeneral.gov/Page-Attachments/ImmigrationLawGuidancetoLawEnforcement.pdf
[39] 725 ILCS 167/25(d).
[40] These best practices are based on Community Oriented Policing Services, Department of Justice, Police Executive Research Forum, *Roadmap to Implementing and Effective Unmanned Aircraft System (UAS) Program*, available at https://www.policeforum.org/assets/UASRoadmap.pdf.
[41] For additional information regarding community engagement and transparency, agencies should review Police Executive Research Forum. 2022. *Community Engagement Strategies for State, Local, Tribal, and Territorial (SLTT) Law Enforcement Unmanned Aircraft System (UAS) Programs*. Washington, DC: Office of Community Oriented Policing Services, available at Community Engagement Strategies for State, Local, Tribal, and Territorial (SLTT) Law Enforcement Unmanned Aircraft System (UAS) Programs (usdoj.gov).

agencies and any individual operators have the necessary federal certifications.[42] Agencies should also review the Illinois-specific requirements imposed by the Act. Finally, agencies should review whether any local ordinances regulate the use of drones.

- **Build a drone team**. Agencies should identify what job positions are necessary to generally maintain a drone program and specifically operate drone missions. The Police Executive Research Forum finds most agencies implementing a drone program employ a "tandem" team, pairing a remote pilot in command with a visual observer.[43] Other team roles could include team leader, camera operator, and safety and security officer. Determine what training is necessary to staff these roles and what certifications those individuals must obtain.

- **Draft the required policy.** The Act requires that a drone program be governed by a publicly available policy. Specific components of a compliant drone policy are described above at Section IV.

- **Draft forms and documents necessary for policy compliance.** The Act requires record keeping for each flight, notification to the State's Attorney for particular flights, and notice to participants prior to the use of a drone to monitor a routed or special event. Agencies should draft form documents to ensure compliance with these requirements and allow for data collection and analysis. They should also ensure that information collected is destroyed in accordance with the timelines set by the Act.

- **Establish record-keeping procedures.** Agencies should maintain records demonstrating compliance with the Act, including:

    - Copies of the agency's policy governing the operation, use, administration, and oversight of its drone program;

    - Records showing when each drone flight occurred, why the agency flew the drone, and what information the agency collected, as reported to the ICJIA;

    - Documentation that drone use pursuant to Section 15(3) was reported to the State's Attorney within 24 hours of the drone flight; and

[42] For additional information regarding federal regulation of drone use, see Federal Aviation Administration, *Drones in Public Safety: A Guide to Starting Operations* (5 June 2025), available at https://www.faa.gov/uas/public_safety_gov/public_safety_toolkit/Public_Safety_BVLOS_OOP_OOMV_Waiver_June_2025.pdf.

[43] Police Executive Research Forum. 2022 (cited in footnote 41) at 29.

- Copies of all notices posted in advance of drone use at a routed or special event, pursuant to Section 15(10).

- **Create First Amendment guardrails.** The Act does not permit agencies to use the special or routed event exception to surveil First Amendment protected activity, although drones may be used under other exceptions under Section 15 of the Act.[44] To ensure compliance with these requirements, agencies should implement policies and practices to ensure drones are not used unlawfully at events with First Amendment activity.

VIII. What is the Office of Attorney General's role in ensuring law enforcement agencies comply with Illinois law regarding drone use?

OAG is committed to ensuring law enforcement agencies comply with the Act's transparency requirements and privacy protections. OAG has express authority under the Act to conduct investigations into patterns and practices of violations of the Act.[45] Such authority includes the right to request written statements under oath, conduct examinations, and issue subpoenas.[46] Furthermore, the Act expressly permits OAG to compel compliance with an investigation through legal action in the circuit court.

Examples of violations of the Act may include, but are not limited to, the following:

- Failing to implement and make publicly available a policy governing the operation, use, administration, and oversight of an agency's drone program;

- Using a drone equipped with a firearm, weaponized laser, kinetic impact projectile, chemical agent or irritant, or any other lethal or non-lethal weapon;

- Using onboard facial recognition software during a drone flight;

- Using a drone at a "routed event" or "special event," as those terms are defined by the Act, without posting a notice at the event location for at least 24 hours before the event that clearly indicates that drones may be used;

- If the agency owns one or more drones, failing to submit an annual written report containing the required information to the ICJIA by April 1, including the specific Section 15 exception that applied to each instance of drone use;

[44] For example, while political protests are not special events which may be monitored pursuant to Section 15(10), the Act permits law enforcement to use a drone to prevent imminent harm to life under Section 15(3), even at a political protest, if warranted under the specific circumstances.
[45] 725 ILCS 167/45(b).
[46] *Id.*

- Using a drone solely to gather information about people engaged in lawful, First Amendment protected activity, such as a lawful demonstration, protest, or march, unless a Section 15 exception applies;

- Using a drone to inspect private locations solely for violations of local ordinances, unless a Section 15 exception applies; and

- Using a drone to gather information on routine patrols of city neighborhoods, unless a Section 15 exception applies.

Following the completion of an investigation, OAG may maintain an action in the circuit court against any law enforcement agency, law enforcement official, or any other person of entity who violates any provision of the Act.[47]

If OAG demonstrates a pattern or practice of violations of the Act and obtains an adverse judgment under the Act, a law enforcement agency shall forfeit its ability to use drones for not less than six months for a first adverse judgment and up to one year for a second adverse judgment.[48]

IX. How can community members and law enforcement report violations of the Act?

As drone technology continues to evolve, law enforcement agency drone use must comply with Illinois law.

Any agency, resident, or other interested party, including those with information regarding suspected practices in violation of state law, is encouraged to contact OAG's Civil Rights Bureau using the contact information below:

- Call the Civil Rights Hotline at (877) 581-3692;

- Email a Civil Rights Complaint Form to civilrights@ilag.gov; or

- Mail or deliver in-person a Civil Rights Complaint Form to the OAG's Chicago office: 115 S. LaSalle Street, Chicago, IL 60603.

KWAME RAOUL
Attorney General
State of Illinois

[47] 725 ILCS 167/45(c).
[48] 725 ILCS 167/45(d).