AN ACT concerning the use of cell site simulator devices.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Citizen Privacy Protection Act.

Section 5. Definitions. As used in this Act:

"Cell site simulator device" means a device that transmits or receives radio waves to or from a communications device that can be used to intercept, collect, access, transfer, or forward the data transmitted or received by the communications device, or stored on the communications device, including an international mobile subscriber identity (IMSI) catcher or other cell phone or telephone surveillance or eavesdropping device that mimics a cellular base station and transmits radio waves that cause cell phones or other communications devices in the area to transmit or receive radio waves, electronic data, location data, information used to calculate location, identifying information, communications content, or metadata, or otherwise obtains this information through passive means, such as through the use of a digital analyzer or other passive interception device. "Cell site simulator device" does not include any device used or installed by an electric utility solely to the extent the device is used by that utility to

measure electrical usage, to provide services to customers, or to operate the electric grid.

"Communications device" means any electronic device that transmits signs, signals, writings, images, sounds, or data in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.

"Law enforcement agency" means 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 criminal laws.

Section 10. Prohibited use of cell site simulator devices. A law enforcement agency may not use a cell site simulator device, except to locate or track the location of a communications device or to identify a communications device. Except as provided in Section 15 of the Freedom From Location Surveillance Act, a court order based on probable cause that a person whose location information is sought has committed, is committing, or is about to commit a crime, is required for any permitted use of a cell site simulator device.

Section 15. Application for court order.

(a) An application for a court order to use a cell site simulator device, including an emergency application under subparagraph (B) of paragraph (6) of Section 15 of the Freedom From Location Surveillance Act, must include:

(1) a description of the nature and capabilities of the cell site simulator device that will be used and the manner and method of its deployment, including whether the cell site simulator device will obtain data from non-target communications devices; and

(2) a description of the procedures that will be followed to protect the privacy of non-targets during the investigation, including the deletion of data obtained from non-target communications devices.

(b) If the cell site simulator device is used to locate or track a known communications device, all non-target data must be deleted as soon as reasonably practicable, but no later than once every 24 hours.

(c) If the cell site simulator device is used to identify an unknown communications device, all non-target data must be deleted as soon as reasonably practicable, but no later than within 72 hours of the time that the unknown communications device is identified, absent a court order preserving the non-target data and directing that it be filed under seal with the court. The court may retain data obtained from a non-target communications device under a court order showing good cause for no longer than the period required under Supreme Court Rules. The law enforcement agency is prohibited from accessing data obtained from a non-target communications device for the purpose of any investigation not authorized by the original court order.

(d) A court order issued under this Section may be sealed upon a showing of need, but for no more than 180 days, with any extensions to be granted upon a certification that an investigation remains active or a showing of exceptional circumstances.

Section 20. Admissibility. If the court finds by a preponderance of the evidence that a law enforcement agency used a cell site simulator to gather information in violation of the limits in Sections 10 and 15 of this Act, then the information shall be presumed to be inadmissible in any judicial or administrative proceeding. The State may overcome this presumption by proving the applicability of a judicially recognized exception to the exclusionary rule of the Fourth Amendment to the U.S. Constitution or Article I, Section 6 of the Illinois Constitution to the information. Nothing in this Act shall be deemed to prevent a court from independently reviewing the admissibility of the information for compliance with the aforementioned provisions of the U.S. and Illinois Constitutions.