The Chicago Council of Lawyers Supports
Illinois Bills Regulating Law Enforcement's use of "Stingrays"

The Chicago Council of Lawyers urges the Illinois General Assembly to pass either of two bills that would regulate the government's use of cell phone simulators, sometimes called "stingrays." The Bills are House Bill 4470, introduced by Representative Williams, and Senate Bill 2343, introduced by Senator Daniel Biss.

I. Background

A cell site simulator, sometimes called a "stingray" is a surveillance device that mimics cell phone towers. The device tricks cell phones within its range to connect to it, instead of to legitimate towers. The government usually obtains the identifying number of a particular cell phone (sometimes called the "target" phone) and its general direction, but in the process, it also collects identifying information from all other cell phones in the area. And it does so without notifying those phone users or their service providers. Moreover, stingray technology makes it possible to obtain the content of a cell phone conversation.

The City of Chicago and other law enforcement agencies in Illinois use stingray technology. They do so at times without seeking a warrant or a court order. When a warrant or judicial order is sought, the nature of the technology is sometimes obscured by the use of technical terminology, such as asking to use a "digital analyzer" device. Before September 3, 2015, the U.S. Department of Justice (DOJ) also used stingray technology without a warrant. When DOJ used this technology jointly with state or local law enforcement agencies, it required them to keep secret their use of such technology. On September 3, 2015, the DOJ published a policy stating that in the future it would usually seek warrants from judges before using cell site simulators. The DOJ policy reserves the right to use this technology without seeking a warrant in emergencies, including to protect human life or avert serious injury; to prevent the imminent destruction of evidence; to pursue a fleeing felon; and to locate fugitives. The DOJ policy limits s the actions of other governments only when it conducts joint investigations with them. The DOJ policy can be reversed by the Obama administration, or by any future President.

II. The Provisions of the Illinois Bills

Section 1 of each bill provides that it will be called "The Citizen Privacy Protection Act." Section 5 of each bill provides for identical definitions of such terms as "cell site simulator device" and "law enforcement agency," the latter term referring to police agencies of Illinois or its subdivisions.

Section 10 of each bill provides that law enforcement agencies may use cell site simulators only to locate, identify or track a particular communication device. Both require the agencies to obtain a warrant based on probable cause, except as provided in Section 15 of the Illinois "Freedom from Location Surveillance Act," (Illinois Public Act 098-1104.)

Section 15 of each bill requires that an application for a court order to use a cell site simulator include a description of the nature and capabilities of the device, the manner and method of deployment, and describe whether the device will capture data of non-target devices. HB 4470 requires that the application describe the procedures to be followed to protect the privacy of non-targets, including the immediate deletion of non-target data. SB 2343 requires that non-target data be deleted within 24 hours when a simulator is used to locate or track a known communication device, and within 72 hours when a simulator is used to identify an unknown communication device. SB 2343 also provides that an order to use a cell site simulator may be sealed under certain circumstances.

Section 20 of each bill provides that if a law enforcement agency uses a simulator to gather information in violation of the limitations set forth in Sections 10 and 15, then the information is inadmissible in any proceeding unless the agency proves an exception to the exclusionary rule of the Fourth Amendment of the U.S. Constitution or the Sixth Amendment of the Illinois Constitution.

As noted above, the exceptions to the requirement that a law enforcement agency first obtain a court order based on probable cause are those specified in Section 15 of the Illinois Freedom From Location Surveillance Act. Some of those exceptions are:

* To aid in the location of a missing person;
* To protect an investigative or law enforcement officer.
* An investigation of abduction;
* Conspiratorial activities characteristic of organized crime;
* An immediate threat to national security;
* A felonious attack on a computer;
* A clear and present danger of imminent death or great bodily harm exists when (a) persons are kidnapped or held hostage forcibly or by the threat of force; or (b) any place, vehicle, vessel or aircraft is occupied by force or threat of force.

III. Both Bills Protect The Privacy of Cell Phone Users.

Cell site simulators hijack information from both targeted and non-targeted cell phones. They can and have been used without a warrant.

Both HB 4470 and SB 2343 limit simulators to locating, identifying or tracking a particular communication device.

Both bills, with specified exceptions, require law enforcement agencies to obtain a warrant based on probable cause, before using a simulator.

Both bills require that an application for a warrant describe whether the device will capture data of non-targeted devices.

Both bills require that information obtained from non-targeted devices be promptly

deleted (within 72 hours at the latest).

Although both bills could be improved, each bill provides substantial protection to the privacy of Illinois cell phone users.. The Illinois General Assembly should protect Illinois cell phone users by passing either HB 4470 or SB 2343