Illinois Should Regulate the Government's use of "Stingray" Technology
Gordon Waldron and Thomas C. Hallock

I. Introduction

On January 20, 2016, Illinois House Representative Ann Williams of Chicago introduced House Bill 4470 to regulate the use by governmental bodies of cell site simulator devices. A similar measure is being introduced in the Illinois Senate under the sponsorship of Senator Daniel Biss.

A cell site simulator, sometimes called a "stingray" is a surveillance device that mimics the towers to which cell phones connect. 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 judicial 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 simulator technology. 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 its own actions but limits the actions of other governments only when it conducts joint investigations with them.

II. The provisions of House Bill 4470, the Citizen Privacy Protection Act

House Bill 4470, the Citizen Privacy Protection Act, would:

*Allow law enforcement to use cell site simulators for the narrow purpose of locating or identifying a particular communication device, after obtaining a court order based on probable cause. (Section 10.)

* Require a court order to include a description of the nature and capabilities of the device, the manner and method of deployment, describe whether the device will capture data of non-target devices, and describe the procedures to be followed to protect the privacy of non-targets, including the deletion of non-target data. (Section 15.)

* Mandate that any data collected beyond the scope of the warrant must be immediately and permanently deleted. (Section 15.)

House Bill 4470 contains exceptions to its requirement that governments first obtain a court order based on probable cause that the targeted person has committed or is about to commit a crime. The exceptions are those specified in Section 15 of the Illinois Freedom From Location Surveillance Act. (Illinois Public Act 098-1104.) Some of those exceptions are:

* To aid in the location of a missing person;
* The cell site simulator is needed 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. Comments on House Bill 4470

The use by law enforcement agencies of cell site simulators without a warrant or by obtaining a warrant without clearly identifying the information sought probably violates the Fourth Amendment rights of the targeted cell phone users, and of other persons whose cell phones are tricked into providing identifying information to the cell site simulator device.

House Bill 4470 thus fills a vital need to regulate the use of cell site simulators. We recognize that incorporating exceptions from an existing statute (the Illinois Freedom From Location Surveillance Act) makes it more likely that House Bill 4470 will pass. Nevertheless, we suggest that the following revisions be made, many of which we think are uncontroversial.

* To enforce the requirement that data collected beyond the scope of the warrant be deleted, the bill should require the filing of an affidavit with the court that such data has been deleted.

* Law enforcement agencies should be prohibited from using the acquired data beyond that necessary to determine the cell phone information of the target.

* The Bill should provide a monetary remedy to persons whose information is obtained, used, or made public in violation of the legislation.

* The exception covering "conspiratorial activities characteristic of organized crime" is vague and overbroad. Accordingly, it should be narrowed to apply only when it is not feasible for law enforcement to seek a court order based on probable cause.