Written by **Joe Wolverton, II, J.D.** on July 29, 2016

New Illinois Law Nullifies Expansion of Surveillance State

A new law in Illinois works to protect citizens of that state from being subjected to electronic surveillance that violates their right to be free from unreasonable searches on the part of government. The statute also serves to restrict the capacity of the federal government to extend the borders of the federal surveillance state within the sovereign borders of Illinois.

Governor Bruce Rauner signed the bill outlawing the use of "Stingray" tracking devices used to monitor and record the location of phones and record critical electronic data of cellphone users, all of which is typically done without a warrant, in direct violation of the rights protected by the Fourth Amendment.

The Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The new state law — known as the Citizen Privacy Protection Act — provides that a cell site simulator device ("Stingray") can only be used to track the position of a person who "has committed, is committing, or is about to commit a crime" and then only if such an action is taken pursuant to "a court order based on probable cause."

Having the eye of justice look over the shoulder of law enforcement is a great boon to the protection of liberty, as it works to prevent overzealous police from using the electronic tracking technology to collect data from people who have not been afforded due process.

Even the process of applying for a court order to grant the use of a Stingray device is subject to very specific guidelines in the new Illinois law.

As part of the petition for a court order, the requesting officer or agency "must include a description of the nature and capabilities of the cell site simulator device to 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."

Those whose signals are caught in the device's electronic net, but who are not the intended targets, are provided particular protection in the new law.

Law enforcement is required to "include a description of the procedures that will be followed to protect the privacy of non-targets of the investigation, including the immediate deletion of data obtained from non-target communications devices."

That's a remarkable reinforcement of the constitutional barricade of privacy — one not present in most similar measures being considered by lawmakers in other states.

The measure's chief sponsor was state senator Daniel Biss, who spoke earlier in the year about the purpose for his proposal. "As advances in technology enable police to more efficiently investigate and solve crimes, it's important that we help them to know they are following state law and the parameters of the Constitution," Biss said.

"Additionally, we must adopt measures that help to ensure privacy for citizens who have done nothing wrong but may find that data from their cell phones was collected and stored by law enforcement for no legitimate legal reason."

Potential problems with the use by law enforcement of a tool as powerful as the Stingray demand an extra measure of vigilance regarding the device's widespread purchase by police.

The function of the technology reveals its threat to the liberties of the law-abiding. The suitcase-sized Stingray masquerades as a cell tower to trick cellphones into connecting to it. It can give police tracking identifiers for phones within a mile or more, depending on terrain. Given the mobility of the device, police who use it can triangulate a target's location with better accuracy than if they relied on data transferred by traditional cell towers.

This equipment isn't cheap. According to published reports, each Stingray device costs about $350,000. Despite the cost, however, it has been reported that nearly 30 police departments admit to owning a Stingray, with about 50 other cities refusing to disclose whether or not they own one of these expensive surveillance devices.

Perhaps because of the cost, but more likely because of the devastating effect on the personal liberty of those caught in the Stingray's net, police and the feds seem to be zealous about keeping the device's deployment a secret.

There is another aspect of the use of Stingray devices that merits attention: The powerful technology employed by the device is dangerous, privacy advocates argue, because it is impossible to restrict the signals tracked by the Stingray to only those users who are suspects and have them receive requisite due process. With these cell-site simulators, every cellphone within range of the device's scan is captured.

If that "non-target" data is not instantly and permanently destroyed, there is a chance that the information could end up in a database of such information that is shared among local law-enforcement agencies and federal bureaus.

Information gathered and given out in this manner is part of a network known in law-enforcement parlance as "information sharing environment" or ISE.

According to its website, the ISE "provides analysts, operators, and investigators with information needed to enhance national security. These analysts, operators, and investigators … have mission needs to collaborate and share information with each other and with private sector partners and our foreign allies." In other words, ISE serves as a conduit for the sharing of information gathered without a warrant.

The constitutional issues aside, such a scheme allows the federal government not only to seduce state and local law enforcement to cooperate with them in their drive to place all Americans under the watchful eye of Washington, D.C., through the proffer of funds necessary to purchase the Stingrays, but

it simultaneously facilitates the creation of a massive database of useful electronic information of every American and the feds get the states and cities to do the dirty work of collecting it all in violation of the Fourth Amendment.

In light of the provisions of the new law, there is hope that Americans residing within the Land of Lincoln will no longer be subject to such denials of their civil rights and that the federal government's efforts to collect and catalog information on every person in this country will be stymied, at least within the borders of Illinois.

The law goes into effect on January 1, 2017.