Written by **Joe Wolverton, II, J.D.** on May 23, 2016

Illinois Lawmakers Unanimously Pass Ban on Unwarranted Stingray Surveillance

On May 18, the state legislature of Illinois passed a bill all but absolutely banning the warrantless deployment of Stingray cellphone surveillance devices in the Land of Lincoln.

The text of Senate Bill 2343 mandates that "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 Stingray or similar tracking tool.

Remarkably in this era of nearly unrestrained growth of the American surveillance state, both chambers of the Illinois state legislative branch passed the measure unanimously.

In what seems to be a very expansive and praiseworthy provision, the act requires that "an application for a court order to use a cell site simulator device, including an emergency application under the Freedom From Location Surveillance Act, 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."

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 bill's chief sponsor was state senator Daniel Biss, who spoke earlier 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."

The Constitution's primary protection of a person's papers and private information is the Fourth Amendment, which 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 Illinois bill seems to satisfy these constitutional requirements.

Potential problems with the use by law enforcement of a tool as powerful as the Stingray demand an extra measure of vigilance on 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 are zealous about keeping the device's deployment a secret.

The secrecy isn't all from the state's side, though.

A *New York Times* article in March of 2015 summarized the surveillance situation in many police departments:

> A powerful new surveillance tool being adopted by police departments across the country comes with an unusual requirement: To buy it, law enforcement officials must sign a nondisclosure agreement preventing them from saying almost anything about the technology.
>
> Any disclosure about the technology, which tracks cellphones and is often called StingRay, could allow criminals and terrorists to circumvent it, the F.B.I. has said in an affidavit. But the tool is adopted in such secrecy that communities are not always sure what they are buying or whether the technology could raise serious privacy concerns.

On April 15, 2015 *CNNMoney* reported on one example of the FBI working with a county sheriff's office to squelch any possible leak regarding the Stingray's use:

> The FBI has a secret device to locate criminal suspects, but they would apparently rather let suspects go free than reveal in court the details of the high tech tracker.
>
> The device, called a "Stingray," tricks cell phones into revealing their locations. Closely guarded details about how police Stingrays operate have been threatened this week by a judge's court order.
>
> Judge Patrick H. NeMoyer in Buffalo, New York, described a 2012 deal between the FBI and the Erie County Sheriff's Office in his court order Tuesday. The judge, who reviewed the deal, said the FBI instructed the police to drop criminal charges instead of revealing "any information concerning the cell site simulator or its use."
>
> Erie police had long tried to keep that contract secret, but the judge rejected that idea and ordered that details of the Stingrays be made public.
>
> "If that is not an instruction that affects the public, nothing is," NeMoyer wrote.

In light of these details on the disturbing uses being made of the Stingray, there are those who argue that the devices' downsides are too large to fit inside the framework of the Fourth Amendment. Here's the Tenth Amendment Center's take on the conflict:

> Some privacy advocates argue that stingray use can never happen within the parameters of the Fourth Amendment because the technology necessarily connects to every electronic device within

> range, not just the one held by the target. And the information collected by these devices undoubtedly ends up in federal data bases. The feds can share and tap into vast amounts of information gathered at the state and local level through a system known as the "information sharing environment" or ISE.
>
> In other words, stingrays create the potential for the federal government to track the movement of millions of Americans with no warrant, no probable cause, and without the people even knowing it.

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.

In the case of SB 2343, an amendment to the original version of the bill proposed by the state's Senate Judiciary Committee reinforced the wall of protection around the personal data of private citizens not suspected of committing any crime (known in the argot of the surveillance community as a "non-target") by requiring that "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."

As of the time of publication of this article, the bill sits on the desk of Illinois Governor Bruce Rauner. Per the process set out in the Illinois state constitution, if the governor does not veto the bill, the bill becomes law with or without his signature 60 days after it is presented to him by the state legislature.

A message left at the governor's office by *The New American* has not been returned.