Written by **C. Mitchell Shaw** on September 4, 2015

New DOJ Policy Restricts Use of Cellphone Spying Tools

On Thursday, the U.S. Department of Justice (DOJ) announced a new policy regarding the way law enforcement can use cell-cite simulators. The new policy requires all federal law enforcement agencies to obtain a warranty before using the devices — known as Stingrays. Though the policy applies to all federal agencies and any state or local agency using these devices, adherence to the policy's warrant requirement is voluntary for all but federal agencies.

As *The New American* reported last week, police departments across the country have been using Stingrays to capture information from cell tower traffic from the innocent and the guilty alike. From that article:

> The Stingray — which is about the size of a large suitcase — is transported in either a surveillance van or a police car. It acts as a "man-in-the-middle" by mimicking a cell tower and fooling any mobile phone in the area into connecting to it. It then harvests info from the phone including the number of the phone, the number the phone is calling or texting, the location of the phone, and information about the phone itself. Once the Stingray has that information, it relays the connection to the nearest real tower in the area. The only things that might alert a mobile phone user to the "man-in-middle" attack by a Stingray would be a sudden dip in battery power or a slight delay in network speeds. The Stingray sends a command to the phone to increase antennae power to maximum, and it takes an extra bit of time to grab what it wants and forward the connection to a real tower.

Because of non-disclosure agreements with with the FBI — which police departments are required to sign in order to obtain these devices — police cannot even disclose how they have used the Stingrays they have. In multiple cases where arrests were made using cell-cite simulators, police have dropped all charges rather than disclose the use of the device. Because police departments do not disclose the use of Stingrays, they rarely obtain a warrant for their use. As we said in the previous article:

> Often there is no search warrant obtained for their use — a direct violation of the Fourth Amendment's guarantee of freedom from "unreasonable searches and seizures" and the requirement that police have "probable cause, supported by Oath or affirmation" to obtain a warrant which must "particularly [describe] the place to be searched, and the persons or things to be seized."

Also, because Stingrays have the ability to capture and record all cell tower traffic — including voice, text, and Internet communications — the new DOJ policy restricts their use to "pen register" mode which allows the device to capture only the location and number of the phone and the numbers the phone is calling or texting. Again, adherence to this policy is voluntary for state and local police agencies.

Less than one week after we reported on the use of Stingrays by at least 50 police departments across

the country, the DOJ has acted to restrict their use and require that all federal agencies obtain a warrant supported by probable cause before using one of these devices to capture cell traffic. Unfortunately, these devices do not discriminate. They work by capturing all traffic to and from cell towers. That means that even if police are "targeting" a particular phone, the traffic from all phones is captured. The policy attempts to deal with this by requiring that in some cases federal agencies must delete all traffic from non-targeted phones within 24 hours while allowing up to 30 days in other cases.

While this is a victory, it is only a small one. Since the new DOJ policy does not do away with the non-disclosure agreements, and is not binding on state and local police agencies, there is little to assure citizens that those police agencies will change anything about the way they are using Stingrays. As the AP reports, "The policy applies only to federal agencies within the Justice Department and not, as some privacy advocates had hoped, to state and local law enforcement whose use of the equipment has stirred particular concern and scrutiny from local judges."

Also concerning to constitutionalists and privacy advocates, the warranty requirement is waived in the event of immediate national security threats and as-yet undefined "exceptional circumstances." As the architects of the culture of surveillance have shown time and again, they are so enamored with the ability to spy on all that citizens do and say, that vaguely worded exceptions quickly become the norm.

Citizens concerned about privacy and transparency in government need to bring hard, fast, steady pressure to bear on their state legislators to forbid the practice of state and local police entering into non-disclosure agreements of this type. They should also demand real protections against such surveillance by all levels of law enforcement.