The New York Times | http://nyti.ms/1LhYJ1R

U.S.

Covert Electronic Surveillance Prompts Calls for Transparency

By **TIMOTHY WILLIAMS** SEPT. 28, 2015

Law enforcement officials across the United States have become enamored of the StingRay, an electronic surveillance device that can covertly track criminal suspects and is being used with little public disclosure and often under uncertain legal authority. Now, though, some states are pushing back, and are requiring the police to get a court order and local consent before turning to the high-tech tool.

Washington, Utah and Virginia recently approved laws requiring court orders for the use of such cell-site simulators by state and local police officers. California lawmakers this month approved such legislation by a wide margin. The California law would also require police agencies to get City Council approval before employing the devices, and to disclose on an agency website that they use the technology. Similar bills have been introduced in Texas and in Congress.

In Maryland, defense lawyers are re-examining thousands of cases to determine if the police have been deploying the technology legally.

“The public has finally become aware of what sorts of technologies are being used, and they are asking themselves, ‘Do we want to pay for this?’ and second,

'What are the costs of this to our civil liberties?' " said Neil Richards, a law professor at Washington University in St. Louis who studies privacy issues. "People do care about privacy. And it is reassuring that the system is working the way it's supposed to — instead of law enforcement just saying, 'The rules have changed when it comes to digital.' "

StingRays, one of several brands of such devices, are about the size of a suitcase. They mimic cellphone towers by forcing mobile phones in their vicinity to connect to the device, which allows the police to find the person with the phone.

The Federal Bureau of Investigation and local law enforcement officials say the devices are critical in locating dangerous criminal suspects. But the devices, which cost as much as $500,000, also collect data from all other cellphones in the area, whether those phones are on or off, without notifying phone users.

The F.B.I., which helps manage the distribution of the devices to police departments, requires agencies to sign nondisclosure agreements prohibiting them from discussing their use of the technology. In recent trials in Missouri and Maryland, prosecutors abruptly dropped cases after police officers declined to testify about the role the devices played in the arrests, according to lawyers and privacy advocates.

But after repeated criticism from members of Congress about the secret use of the technology, the Justice Department this month announced new guidelines that in most circumstances require F.B.I. and other federal agents to obtain search warrants before they use StingRays and prohibit agents from using the devices to collect emails, texts and other data from cellphones. Data obtained from the bystanders' phones must be discarded at the end of each day.

The surveillance devices "are a really critical tool for us that we use in a variety of contexts," said Sally Q. Yates, the deputy attorney general at the Justice Department, at a news conference this month announcing the new guidelines. "There's a real legitimate interest in not letting out the details of exactly how this works so sophisticated criminals and organizations can't then figure out how to

defeat it."

"Would it be better for law enforcement if we didn't give up any of this information?" she continued. "Yeah, it probably would. But there's also an interest in transparency and in public confidence as well. We're trying to find the balance."

The directive does not cover local police departments, where agencies in at least 21 states use StingRays or similar devices, according to the American Civil Liberties Union.

In a 2008 case in Florida, the Tallahassee police used a StingRay or a similar device to find James L. Thomas in a housing complex. The police suspected him of raping a woman and stealing her purse, which contained the woman's cellphone.

"Using portable equipment, we were able to actually basically stand at every door and every window in that complex and determine, with relative certainty you know, the particular area of the apartment that that handset was emanating from," a police officer testified, according to court records.

But when Mr. Thomas's girlfriend opened the door and asked whether the officers had a search warrant, they forced their way inside, according to court documents. The police department later said it had not obtained a search warrant because officers did not want to reveal their use of the technology; they had signed a nondisclosure agreement with the F.B.I., according to the court records.

Mr. Thomas was convicted of sexual battery and theft. A judge later ruled that the search had been illegal and ordered a new trial.

In Baltimore, the public defender's office said it was examining hundreds, potentially thousands, of cases in which the police used StingRays without telling defense lawyers. In all, the Baltimore police have acknowledged using StingRays 4,300 times since 2007.

Natalie Finegar, the deputy district public defender in Baltimore, said that when defense lawyers pressed for details about how the police located certain

suspects, prosecutions had suddenly been withdrawn to avoid answering questions about StingRays.

"There are cases where it was never spelled out for the judge, and certainly not for us," Ms. Finegar said. "Sometimes they dropped cases and other times they would say, 'We're not going to use that evidence.' We didn't think it was used very often at all. We had no idea."

The United States Supreme Court has not yet taken a case challenging whether the use of StingRays by the police without search warrants violates the Fourth Amendment's protections against unreasonable searches.

But in recent years, the court has ruled that the police must obtain a search warrant to either place a GPS device on a vehicle or to sift through the contents of a suspect's cellphone.

The person who has perhaps been the most successful in pressing for public disclosure about StingRays is a 35-year-old Arizona man who was arrested after federal agents located him using similar technology.

The man, Daniel Rigmaiden, pleaded guilty to tax fraud in 2014; the authorities said he used the names of dead people and others to file $5.2 million in fraudulent tax claims. In an interview this month, he said that after his arrest in 2008, he told a lawyer, "I think they tracked me down by sending rays into my living room."

"In retrospect, I can see how it might sound like something a crazy person might have come up with," Mr. Rigmaiden added.

In his case, it turned it out to be true. At the time, the existence of StingRays was still a closely held government secret.

Soon after, his lawyer — at least his fourth one — withdrew from the case; eventually Mr. Rigmaiden represented himself and spent nearly six years in prison. Before he pleaded guilty, he began researching StingRays, setting up shop in the

prison library and collecting more than 40,000 pages of documents before finding a reference in a government report to the device.

His research helped convince the A.C.L.U. that federal agents had and were using the technology. Since then, the group has led efforts to investigate and change government use of the device. Mr. Rigmaiden volunteered with the A.C.L.U. as part of his community service requirement after his release from prison.

This year, Mr. Rigmaiden, who has become a privacy advocate, helped Washington State write its StingRay law, and he has also taught criminal defense lawyers how to challenge the use of the technology, the A.C.L.U. said.

In Utah, Ryan Wilcox, a former Republican state legislator who sponsored that state's StingRay law, said in an interview that he had been able to convince his colleagues of the potential danger of the warrantless use of StingRays in a new way: He used equipment he had bought at a local store to project the contents of his cellphone onto a conference room wall.

"Are you comfortable having all your information — your contacts, your appointments, your photos — this easy to access?" he asked them.

The legislation passed overwhelmingly.

A version of this article appears in print on September 29, 2015, on page A12 of the New York edition with the headline: Covert Electronic Surveillance Prompts Calls for Transparency .