



What Is the Future of the Fourth Amendment Under Trump?

June 22, 2017

Law enforcement uses tracking devices called “stingrays” to locate cellphones. But the technology also picks up personal information from other c...

Law enforcement agencies say Stingray technology helps them catch suspected criminals — and it does. But privacy advocates fear the technology’s ability to collect nearby cell phone owners’ data without their permission or knowledge — and often, without a warrant — compromises Fourth Amendment rights.

Federal authorities have said the devices they use are not configured to collect the content of communications, but the capabilities of the technology aren’t clear. That’s partly because federal authorities have shrouded cell site simulators in mystery, sometimes dropping cases against criminal suspects rather than reveal their policing methods and agreements with private cell site simulator companies that swear the government to product secrecy in contracts.

The ability to put the warrant requirement “through the shredder” at any moment is why policy is an insufficient safeguard, said Matthew Feeney, policy analyst at the Cato Institute, a libertarian think tank.

“We’re relying heavily on government policy rather than law, and that I think is a problem,” Feeney said.

Many states also use automatic license plate readers, technology that can scan hundreds of plates per minute. In the 2008 election cycle, Virginia State Police used automatic license plate readers on attendees’ cars at political rallies for Barack Obama and Sarah Palin, the ACLU revealed. Alone, license plates may not amount to much information, but police have the ability to check those plates against other records, and — over time — can observe patterns about a driver’s habits, the ACLU argued.

Meanwhile, the federal government is quietly ramping up its surveillance approach at airports, using technology that was, “in most cases developed for the battlefield,” Bedoya said.