House Oversight Committee

May 13, 2014

My name is Brian Owsley and I want to thank you for having me address you this morning. I am currently a Visiting Assistant Professor of Law at the Texas Tech University School of Law and in the coming academic year will be an Assistant Professor of Law at the Indiana Tech Law School. Previously, I served as United States Magistrate Judge for the Southern District of Texas.

I am going to address the Government's use of cell site simulators from my perspective as a former federal judge as well as an academic. I will often use the term StingRay, which is a specific mode of a cell site simulator manufactured by the Harris Corporation, as a generic reference.

The first time that I ever dealt with a StingRay was in April 2011. I received a pen register application filed by an Assistant United States Attorney alleging that some federal inmates were suspected of using cell phones to engage in federal crimes at the Federal Corrections Institution in Three Rivers, Texas. Although the Government knew who these inmates were, they did not know the cell phone numbers. Hence, they filed the pen register application, which essentially seeks authorization of a list of all telephone numbers that are outgoing from a given telephone.

Although it was captioned as a pen register, the application sought to use a device that would capture any cell phone used within the vicinity of the prison. In other words, this did not sound like a pen register. In a hearing with the Assistant United States Attorney, I sought more information, including some briefing that the pen register statute applied to such a request. It was also acknowledged that other cell phones besides the target cell phone being used by the inmate would be captured by the StingRay device. I was told that the briefing would be forthcoming.

After that hearing when I would see the Assistant United States Attorney, I would periodically ask about the status of the briefing memorandum that I had been promised. Each time, I was told that I could expect it shortly. However, after a month or so, I was advised that shortly after the application for the pen register was filed, prison officials located the cell phone and seized it. Because there was no longer a need for the pen register, I denied the application as moot. I am not sure that I would have ever received the briefing memorandum. It is my understanding that most of that type of legal analysis would not be done locally, but instead come from Department of Justice attorneys.

The second time that I dealt with a StingRay as a magistrate judge was about a year later. A DEA agent again filed a pen register application in a narcotics trafficking investigation, but the Government did not have a cell phone number. During a hearing to discuss the application, the agent admitted that he was proposing to use a StingRay. If I granted the application, he would

drive around in a vehicle near the home of the targeted person using the device hoping to capture the person's cell phone number. He would also follow the subject to other locations and engage in similar surveillance and electronic data capture so that he could possibly narrow down the cell phone number based on a specific number appearing at multiple sites. The Assistant United States Attorney who filed the application indicated that it was based on a standard form provided by the Department of Justice. At the conclusion of the hearing the Assistant United States Attorney promised to provide a legal memorandum supporting the application, but it was never provided.

Ultimately, I denied this second application in a written opinion, *In the Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trace and Trace Device*, 890 F. Supp. 2d 747 (S.D. Tex. 2012). I did so for a couple of reasons. First, I concluded that the pen register statute was inapplicable in part because that statute and subsequent case law analysis envision that an application would present a known cell phone number for which the outgoing calls would be provided. Here, the Government was essentially trying to capture the targeted cell phone number. Instead of the pen register statute, I determined that the Government could only obtain authorization for a StingRay if it satisfied the Fourth Amendment, including establishing probable cause. As part of that analysis, a court must address whether the cell phone users, the targeted individual as well as the innocent bystanders, have a reasonably expectation of privacy in the use of their cell phone. Finally, if an application for a StingRay were to be granted, there needs to be a protocol in order to address all of the innocent bystanders whose electronic data is capture. The Government may be required to notify these people or certify that they have destroy records of the captured electronic data.

There are other examples from other federal courts that I have become aware of in my research. I also have tried to talk with other magistrate judges about these types of applications. I am concerned because the Government's application gives the appearance of a pen register application, which is a very routine matter for a magistrate judge and one that is routinely granted because the standard is so low. The information sought need only be certified as "relevant to an ongoing criminal investigation." I am fear that some magistrate judges who are not technologically savvy or in tune to this issue may simply view the StingRay request as a pen register application and simply sign it authorizing a very invasive procedure.