

WHY ARE THE US MARSHALS AT THE CENTER OF ALL THESE PEN REGISTERS?

The US Marshal Service shows up prominently in two Pen Register stories from yesterday.

First, as part of a great story from WSJ's Jen Valentino-Devries mapping out how many federal criminal electronic records requests never get unsealed..

In eight years as a federal magistrate judge in Texas, Brian Owsley approved scores of government requests for electronic surveillance in connection with criminal investigations—then sealed them at the government's request. The secrecy nagged at him.

So before he left the bench last year, the judge decided to unseal more than 100 of his own orders, along with the government's legal justification for the surveillance. The investigations, he says, involved ordinary crimes such as bank robbery and drug trafficking, not "state secrets." Most had long since ended.

A senior judge halted the effort with a [one-paragraph order](#) that offered no explanation for the decision and that itself was sealed.

She released this summary of all the Federal Pen Register/Trap and Trace requests in 2012. As she pointed out on Twitter, the greatest number of requests don't come from FBI. They come from the USMS, which submitted almost half of all requests that year, with 9,132.

Then, the ACLU revealed that, just before an appointment to view Sarasota, Florida's requests

under the Pen Register authority to use Stingray IMSI catchers to identify cell locations, the US Marshals declared control over the records, claiming they had deputized the local cop who had made the requests.

Over the past several months, the ACLU has filed dozens of public records requests with Florida law enforcement agencies seeking information about their use of controversial cell phone tracking devices known as “stingrays.” (The devices are also known as “cell site simulators” or “IMSI catchers.”) Stingrays track phones by mimicking service providers’ cell towers and sending out powerful signals that trick nearby phones – including phones of countless bystanders – into sending their locations and identifying information.

The Florida agencies’ responses to our requests have varied widely, with some [stonewalling](#) and others releasing records. The most recent request went to the Sarasota Police Department, and the fallout from that request has raised red flag after red flag.

RED FLAG #1: The Sarasota Police initially told us that they had responsive records, including applications filed by and orders issued to a local detective under the state [“trap and trace”](#) statute that he had relied on for authorization to conduct stingray surveillance. That raised the first red flag, since trap and trace orders are typically used to gather limited information about the phone numbers of incoming calls, not to track cell phones inside private spaces or conduct dragnet surveillance. And, such orders require a very low legal standard. As one federal magistrate judge has held, police should be

permitted to use stingrays only after obtaining a probable cause warrant, if at all.

RED FLAG #2: The Sarasota Police set up an appointment for us to inspect the applications and orders, as required by Florida law. But a few hours before that appointment, an assistant city attorney sent an email cancelling the meeting on the basis that the U.S. Marshals Service was claiming the records as their own and instructing the local cops not to release them. Their explanation: the Marshals Service had deputized the local officer, and therefore the records were actually the property of the federal government.

[snip]

RED FLAG #3: Realizing we weren't going to get hold of the Sarasota Police Department's copies of the applications and orders anytime soon, we asked the county court if we could obtain copies from its files. Incredibly, the court said it had no copies. The court doesn't even have docket entries indicating that applications were filed or orders issued. Apparently, the local detective came to court with a single paper copy of the application and proposed order, and then walked out with the same papers once signed by a judge.

Court rules – and the First Amendment – require judges to retain copies of judicial records and to make them available to the public, but the court (and the detective) completely flouted those requirements here.

Valentino-Devries notes that a lot of the records being kept secret also involve cell location.

In 2011, magistrate judges in California complained that investigators were applying for pen registers without explicitly saying they wanted to use sophisticated cellphone-location trackers, called “stingrays,” which can be used to locate suspects. Stingrays gather phone-number information, along with other data transmitted by cellphones, by acting as fake cellphone towers. The 1986 surveillance law doesn’t contemplate such technology.

Mr. Owsley, the former Texas magistrate judge, says he had similar concerns about applications for “[cell-tower dumps](#),” in which agents can obtain records of all phones within range of specified cell towers over time—including people who aren’t suspected of a crime.

While we don’t yet know how many of the 9,000 requests the Marshals made in 2012 were for location data, the coincidence is mighty interesting.

The Marshals do have cause to search for suspects’ location. They claim they arrest over 300 wanted fugitives a day. That’s where stingrays would be particularly useful, as they would help to identify the location of a known suspect.

So how often are the Marshals using stingrays to do their work? And to what degree do they do so hiding behind even more obscure local pen register laws to do so?