Written by **Joe Wolverton, II, J.D.** on July 26, 2012

Judge Criticizes Secret Electronic Surveillance Warrants

I was taught in law school that it is the eye of a judge looking over the shoulder of law enforcement that protects the people's due process rights. That eye, according to one federal judge, is being encouraged to look the other way when it comes to requests for electronic surveillance warrants.

In an interview cited by the *New York Times*, Magistrate Judge Stephen W. Smith reports that he frequently considers requests by law enforcement to monitor the cellphone and e-mail records of citizens. He dutifully carries out this judicial obligation, but he has begun to wonder why such proceedings are kept hidden from the public.

"Courts do things in public," Judge Smith said in the interview quoted by the *Times*. "That's the way we maintain our legitimacy. As citizens, we need to know how law enforcement is using this power."

In an effort to shine a bit of light on a subject he feels is being unnecessarily shrouded from view, Judge Smith has written an article describing (and decrying) the secrecy of a docket that, as the *Times* reporter records, "has no parallels in American history."

As one might imagine, gathering the relevant research needed to write such an exposé was not easy. Judge Smith is quoted as saying that "even judges have difficulty finding out what other judges are doing." Some of that activity is being discovered, however.

Recently, *The New American* covered a few stories that pull the blanket of secrecy off law enforcement's efforts to keep Americans under the government's watchful eye. As we chronicled in a recent article, a report issued by cellphone carriers indicated that last year, they received 1.3 million demands from "law-enforcement agencies" for access to the text messages and locations of subscribers to the cellphone companies' service.

An article covering the report was published by the *New York Times* and provided the following breakdown of the requests for information received by the various cell companies:

> AT&T alone now responds to an average of more than 700 requests a day, with about 230 of them regarded as emergencies that do not require the normal court orders and subpoena. That is roughly triple the number it fielded in 2007, the company said. Law enforcement requests of all kinds have been rising among the other carriers as well, with annual increases of between 12 percent and 16 percent in the last five years. Sprint, which did not break down its figures in as much detail as other carriers, led all companies last year in reporting what amounted to at least 1,500 data requests on average per day.

As for the police, they insist that using a cell signal or a record of text messages or data received or sent using a phone makes tracking a person so much simpler. An interview with a member of law enforcement included in the *Times* article is very enlightening as to the desire on the part of police to

keep this weapon in their arsenal. “At every crime scene, there’s some type of mobile device,” said Peter Modafferi, chief of detectives for the Rockland County district attorney’s office in New York, who also works on investigative policies and operations with the International Association of Chiefs of Police. The need for the police to exploit that technology “has grown tremendously, and it’s absolutely vital,” he said in the interview.

Fair enough. There is undoubtedly legitimate need for the issuing of surveillance warrants. The problem is that those warrants are being issued without probable cause in those instances where police are claiming not to be interested in the content of the information collected. As the *Times* article explains:

> Under the Electronic Communications Privacy Act of 1986 [EPCA], officials do not need to establish probable cause to obtain various kinds of phone and e-mail records if they are not seeking the content of the communications. If all officials want to know is whether someone was near a cellphone tower on a given date, say, or whom that person called or e-mailed last month, the law says the government need only demonstrate to a judge that there are “reasonable grounds to believe” that the information sought is “relevant and material to an ongoing criminal investigation.”

That sort of justification is certainly setting the threshold for “legal” searches and seizures very low, definitely below the standard set out in the Bill of Rights. The Fourth Amendment reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In light of the foregoing information regarding the behavior of law enforcement in obtaining and executing these electronic surveillance warrants, the part of the Constitution requiring that warrants particularly describe the objects of the search is being routinely ignored, and perhaps even more frighteningly, this “ignoring” is routinely approved by judges.

In his article, Judge Smith identifies what he considers the most noxious aspect of the entire broken system:

> Through a potent mix of indefinite sealing, nondisclosure (i.e., gagging), and delayed-notice provisions, ECPA surveillance orders all but vanish into a legal void. It is as if they were written in invisible ink — legible to the phone companies and Internet service providers who execute them, yet imperceptible to unsuspecting targets, the general public, and even other arms of government, most notably Congress and the appellate courts.
>
> Lack of transparency in judicial proceedings has long been recognized as a threat to the rule of law and roundly condemned in ringing phrases by many Supreme Court opinions.

To paraphrase a famous legal maxim: Notice delayed is notice denied. Our nation’s legal system is founded on the right of the individual being accused of a crime to know the nature of the charges, and to have an opportunity to answer those charges before an impartial judge. Institutional secrecy and procedural chicanery on the part of law enforcement is destroying that foundation, however.

Judge Smith points to a critical blow being dealt by law enforcement’s demand of judicial secrecy to another one of our timeless Anglo-Saxon jurisprudential cornerstones: Transparency. On this topic, Smith writes:

> The Court elaborated on the unbroken Anglo-Saxon tradition of public access to criminal

> proceedings in *Richmond Newspapers, Inc. v. Virginia*: "Even without such experts to frame the concept in words, people sensed from experience and observation that, especially in the administration of criminal justice, the means used to achieve justice must have the support derived from public acceptance of both the process and its results."

Finally, Judge Smith suggests that although there are no public records that provide actual figures, Freedom of Information Act requests indicate that "thousands of times every year" those law-abiding citizens whose e-mails, text messages, social media posts, and cellphone calls have been monitored by law-enforcement agents will never know that they have been the target of such secret electronic surveillance. Furthermore, they may never know why.

It seems, then, that when it comes to the power of police to secretly secure constitutionally questionable search warrants to track our every electronic footstep, the bottom line is: What we don't know might be killing us — and the Constitution.