TEACHING CRIMINAL PROCEDURE—ESPECIALLY THE FOURTH AMENDMENT ON ELECTRONIC SURVEILLANCE— TO EVERYONE BUT LAW STUDENTS

BRIAN L. OWSLEY*

I think most people contemplating the teaching of Criminal Procedure envision a scenario involving a classroom. While this thought is quite reasonable, it does not apply to me as I have not as of yet taught Criminal Procedure in a formal classroom. I want to teach the course, but so far my teaching in this area has been targeted toward everyone but law students. The goal in this approach, however, is to influence judicial decisions as well as public policy regarding my particular interest in the interplay between the Fourth Amendment and electronic surveillance. I am honored that the *Saint Louis University Law Journal* found what I have been doing worthy of consideration and inclusion in its issue on *Teaching Criminal Procedure*.

I have been dealing with issues related to Criminal Procedure for the last ten years. In 2005, I became a United States Magistrate Judge for the Corpus Christi Division of the United States District Court for the Southern District of Texas where I first dealt with matters of criminal law and criminal procedure. Since 2013, I have been teaching law, but as I admitted have not yet taught Criminal Procedure. Instead of law students in front of a podium, I have focused on other students, including law enforcement officials, legal practitioners, judges, and legislators, with lessons mostly about the Fourth Amendment and electronic surveillance.

Magistrate judges deal with all manner of applications for surveillance and investigatory purposes, including pen registers,[1] and trap and trace devices;[2] disclosure of a telecommunication subscriber's records or communications;[3] and search warrants.[4] Moreover, they routinely sign criminal complaints[5] and

* Assistant Professor of Law, University of North Texas—Dallas College of Law; B.A., University of Notre Dame; J.D., Columbia University School of Law; M.I.A., Columbia University School of International and Public Affairs. From 2005 until 2013, the author served as a United States Magistrate Judge for the United States District Court for the Southern District of Texas.

1. 18 U.S.C. § 3122 (2012).
2. *Id.*
3. 18 U.S.C. § 2703 (2012).
4. FED. R. CRIM. P. 4.1(a).

issue arrest warrants.[6] These documents are typically presented to a magistrate judge by a federal agent or an assistant United States attorney. One of the first teaching experiences is to ensure that they understand the appropriate standard and file applications consistent with that standard.

Pen registers are surveillance techniques that enable law enforcement officials to obtain a list of *outgoing* calls from a known telephone number from a telecommunications provider.[7] Conversely, trap and trace devices enable them to obtain a list of *incoming* calls from a telecommunications provider based on a known telephone number. Because these are relatively low stakes in terms of the information obtained, the standard set by Congress to obtain authorization is also very low: when an application is filed:

> [T]he court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.[8]

Very rarely, if ever, would a presiding magistrate judge deny a pen register in light of this standard.

An application for a telecommunication subscriber's records and information can obtain a list of information about a cell phone subscriber, including the person's name, date of birth, mailing address, payment method, driver's license number, social security number, and information that locates the person to a specific location.[9] It requires a standard that is higher than a pen register in that the official seeking the court order must "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[10]

These two lesser standards are contrasted with that standard derived from and first enunciated in the Fourth Amendment:

> 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 [w]arrants shall issue, but upon probable cause, supported by [o]ath or

5. FED. R. CRIM. P. 3.

6. FED. R. CRIM. P. 4(d).

7. Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 195 (2014).

8. 18 U.S.C. § 3123(a) (2012).

9. 18 U.S.C. § 2703(c)(2) (2012); *see also* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 15 (2013) (discussing the various obtainable information).

10. 18 U.S.C. § 2703(d).

> affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[11]

In order to obtain a search warrant or a criminal complaint and arrest warrant, the law enforcement officer must demonstrate that there is probable cause that a crime has been committed. Whereas, a pen register or a § 2703(d) order both contain lesser standards falling outside the parameters of a Fourth Amendment search. Consequently, the only protections citizens have regarding those methods of electronic surveillance are what Congress deems appropriate to provide.

Thus, there are essentially three standards magistrate judges may apply regarding applications for electronic surveillance. A problem with dealing with electronic surveillance issues is that courts have received very little guidance from Congress. One of the most significant pieces of legislation is the Electronic Communications Privacy Act (ECPA) that addresses both pen registers and the release of subscriber.[12] That statute was enacted in 1986 and amended by the Communications Assistance for Law Enforcement Act[13] to ensure that telecommunications providers facilitated law enforcements' access to electronic surveillance, and amended again by the USA Patriot Act.[14] However, ECPA has largely dealt with electronic surveillance based on a statute that was enacted just as cell phones were being authorized for consumer use by the Federal Communications Commission.

From my perspective, the education of federal agents and prosecutors stemmed not so much from their lack of knowledge about the various standards in their applications, but instead mostly on their willingness to stretch those standards in inappropriate means. For example, an agent may seek authorization for the use of a cell site simulator, a device that mimics a cell tower and downloads all nearby cell phones that register with it, pursuant to the pen register statute. They seek to use the pen register statute because the standard is very low but ignore the fact that a pen register does not have much to do with the specific type of electronic surveillance that the application proposes, except for the fact that it concerns cell phones. When I received these applications based on the pen register statute, I would open dialogue with the assigned assistant United States attorney as to the statutory authority for the request. I viewed this chance to discuss the issue as an opportunity to educate the person about it.

11. U.S. CONST. amend. IV.

12. Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (1986).

13. Communications Assistance for Law Enforcement Act, Pub. L. 103-414, 108 Stat. 4279 (1994).

14. USA Patriot Act of 2001, Pub. L. 107-56, 115 Stat. 272 (2001); *see also* Owsley, *supra* note 7, at 197–98 (discussing how the Act amended the definition of a pen register and the implications).

In one case, the request involved a cell phone that was being used by inmates in a federal prison pursuant to the pen register statute.[15] My concern was that the statute did not cover this type of request. When I asked the federal prosecutor about the authority for the application, I received assurances that briefing would be provided. This was the mantra for a couple of weeks. Every time I saw the prosecutor, I would inquire about the briefing and was again assured that it would be forthcoming. Eventually, the prosecutor acknowledged that shortly after the filing of the application, prison officials located and seized the cell phone that was the subject of the application. Upon hearing this news, I informed the government that information solved the problem and denied the application as moot. However, I also explained that the original request would have likely been granted if the application were for a search warrant based on probable cause.

About a year later, I had another application for a cell site simulator pursuant to the pen register statute, this time involving a narcotics trafficking investigation.[16] I conducted an *ex parte* hearing regarding the application where I again asked for the statutory authority to support this approach. I was assured that a brief would be forthcoming the next day but, again, that memorandum of law was never filed. Subsequently, I denied the application, finding that the pen register statute was inapplicable and that any such request must be based on a search warrant consistent with the Fourth Amendment.

I had similar experiences in many respects with applications from federal prosecutors seeking a cell tower dump, which essentially permits law enforcement to obtain all of the records from the cell towers in a specific area during a specific time period in order to seek a criminal suspect. The government typically filed these applications pursuant to § 2703 as opposed to a search warrant. Because I concluded that these applications essentially sought to pinpoint the locations of the targeted individuals, I concluded that the appropriate standard was probable cause.[17]

15. Owsley, *supra* note 7, at 203–04.

16. *In re* the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012); *see also* Owsley, *supra* note 7, at 204–05.

17. Prior to publication, two separate circuit splits on whether obtaining historical Cell Site Location Information (CSLI) is a Fourth Amendment search have arisen and disappeared. United States v. Davis, 754 F.3d 1205 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*, 573 F. App'x 925 (11th Cir. 2014), *reh'g en banc in part*, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015); United States v. Graham, 796 F.3d 332, 344 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015). A recent Massachusetts Supreme Court opinion provides an accurate description of the current situation:

> Although the Supreme Court has not considered the issue whether the government's obtaining CSLI from a cellular service provider constitutes a search in the constitutional sense, a number of lower Federal courts have done so. Applying the third-party doctrine articulated in *Miller* and *Smith,* a majority of these courts has ruled that an individual has

After that first cell tower dump application, I had another assistant United States attorney approach me about authorizing a cell tower dump. During an *ex parte* hearing, I asked him whether the application that he had filed was essentially a cell tower dump. After he acknowledged that it was, I asked him whether he had read my most recent order denying a cell tower dump pursuant to § 2703, which apparently he had not. I suggested that we reconvene after he had a chance to read my decision. I explained to him that I would deny his application pursuant to § 2703 for the same reasons that I had in my previous decision.[18] However, I discussed with him that I thought the application could be narrowly tailored in its request in such a manner as to satisfy a probable cause standard. Ultimately, he did re-file his application as a search warrant, and it was granted.[19] I think these applications and the resulting order were a great example of teaching Criminal Procedure insofar as the proper standard was discussed, and ultimately a good outcome for both the Fourth Amendment and the government was achieved. Moreover, this assistant United States attorney went back and in turn educated a number of other attorneys in the office.

Finally, while on the bench, I sought to assist other magistrate judges as well as learn from many of them through various means. Most notably, there would be formal and informal discussions with a number of them. In email exchanges, a number of them indicated that they were unaware of applications for cell tower dumps or cell site simulators. This lack of knowledge is particularly concerning to me as I fear that some magistrate judges may have had an application for a cell site simulator, but instead they just viewed it as an ordinary pen register application and granted it based on that statute's low standard. This type of exchange served as the basis for teaching about the appropriate standards to be employed in such an application. Moreover, it influenced my decision that not only was the pen register statute inapplicable to a cell site simulator, but in the absence of any statutory basis for dealing with this new technology, the appropriate standard was to require the government to demonstrate probable cause and obtain a warrant consistent with the Fourth Amendment.

Since leaving the bench, I have focused my scholarship on writing articles about electronic surveillance and the Fourth Amendment.[20] My target

> no reasonable expectation of privacy in the CSLI because it is a third-party business record, and therefore the warrant requirement of the Fourth Amendment does not apply.

Commonwealth v. Augustine, 4 N.E.3d 846, 857–58 (Mass. 2014).

18. *See In re* Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 964 F. Supp. 2d 674 (S.D. Tex. 2013).

19. *See In re* Search of Cellular Tel. Towers, 945 F. Supp. 2d 769 (S.D. Tex. 2013).

20. Owsley, *supra* note 7; Owsley, *supra* note 9; Brian L. Owsley, *Spies in the Skies: Dirtboxes and Airplane Electronic Surveillance*, 113 MICH. L. REV. FIRST IMPRESSIONS 75 (2015), http://michiganlawreview.org/wp-content/uploads/2015/08/113MichLRevFI75_Ows

audiences for these articles are not only other academics and legal scholars but also judges. Writing for judges is important because in my experience many judges do not always fully understand and appreciate the implications of the orders that they sign. For example, in seeking authorization for the use of a cell site simulator, not only does the government cite and rely on the pen register statute, but they are trained to use a form application and proposed order that appears very similar to a pen register statute.[21] Given the low standard and the lack of familiarity or sophistication regarding some matters related to electronic surveillance, it is quite possible that some judges sign cell site simulator applications believing that they are just pen register applications.

In addition to writing for judges, I also strive to write articles that influence criminal defense attorneys and impact their daily practice. Beyond, the articles that I have noted already, I have written regarding other Fourth Amendment issues[22] as well as I have revised some articles specifically for a publication geared toward practitioners, *Search and Seizure Law Report*.[23] These articles condense law review articles in a manner designed to be more useful to practicing attorneys, which in turn is critical for criminal defense attorneys to understand these new developments in criminal procedure. Given that many of the electronic surveillance issues are dealt with in an *ex parte* manner,[24] these attorneys do not have the direct knowledge and experience that their prosecutorial counterparts do. In order to address some of the issues raised related to prosecutions utilizing electronic surveillance, defense attorneys need to understand these issues. Some are starting to raise the issues in motions to suppress evidence and other motions, but many still are not fully addressing the issues.

Beyond scholarship, I have taken a number of steps toward teaching Criminal Procedure to other audiences. For example, I have also presented at a judicial conference and am working to present at more because this enables me

ley.pdf [http://perma.cc/SX5C-35GA]; Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 AKRON L. REV. 315 (2015).

21. *Compare* U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS 166–70 (rev. June 2005) (form application and proposed order for a pen register, and trap and trace device); *id.* at 171–74 (form application and proposed order for a cell site simulator).

22. Owsley, *Spies in the Skies: Dirtboxes and Airplane Electronic Surveillance*, *supra* note 20; Owsley, *Beware of Government Agents Bearing Trojan Horses*, *supra* note 20; Brian L. Owsley, *The Supreme Court Goes to the Dogs: Reconciling* Florida v. Harris *and* Florida v. Jardines, 77 ALB. L. REV. 349 (2014).

23. Brian L. Owsley, *Cell Site Simulators and the Fourth Amendment*, 43 SEARCH & SEIZURE L. REP. (forthcoming 2016); Brian L. Owsley, *Drug Sniffing Dogs and the Fourth Amendment*, 42 SEARCH & SEIZURE L. REP. 37 (2015).

24. *See generally* Brian L. Owsley, *To Unseal or Not to Unseal: The Judiciary's Role in Preventing Transparency in Electronic Surveillance Applications and Orders*, 5 CALIF. L. REV. CIR. 259 (2014).

to talk to and teach directly with a group that I want to reach. I also have served as a presenter or panelist at other legal academia conferences in order to share my views and thoughts with other legal scholars regarding the Fourth Amendment and electronic surveillance. Just as I rely on many of their articles and ideas to support my scholarship, my hope is that they will do the same with mine, which will in turn influence courts and public policy.

I have also worked with legislators and their staffs to assist them in better understanding electronic surveillance and its constitutional implications. For example, I have spoken with legislative assistants on Capitol Hill about various issues. Moreover, I have testified before a state house committee regarding cell site simulators.[25]

Finally, a group of people that it would not have occurred to me to reach out to before I started teaching is journalists. I talk with and assist them by providing background or quotations regarding a number of topics related to electronic surveillance. This has spread my views and concerns to an extremely wide audience in mainstream media outlets, such as the *Washington Post* and the *Wall Street Journal*, as well as more specialty media. The influence of the media should not be understated. For example, I write much about cell site simulators. When I started doing this a few years ago, there was little being written or discussed about these devices. However, more recently, the media has started writing about them, which in turn has generated significant interest by the public, and concern by politicians and courts. Some legislation limiting the use of cell site simulators without warrants have been enacted by state legislatures. This newly developed interest further enables me to teach about this issue as well as to promote public policy changes.

As I mentioned, I hope to teach Criminal Procedure in a classroom to law students someday. However, I am very satisfied with the teaching of Criminal Procedure that I have been able to do in the last ten years. My hope is that some of the teaching has had an impact on the various target audiences and increased their knowledge about criminal procedure topics. That is what I would hope for in the classroom and that is what I hope for when teaching everyone but law students.

25. *Hearing on Hailstorm/Stingray Type Surveillance Devices Before the H. Oversight Comm.* at 46:50 (Mich., May 13, 2014) (testimony of Brian L. Owsley), http://www.house.mi.gov/MHRPublic/videoarchive.aspx [http://perma.cc/K882-3RSB] (follow "play video" hyperlink for Oversight, Tuesday, May 13, 2014. On most platforms, only the audio plays within the browser. Right click and download to play the video in a stand-alone media player, such as Windows Media Player).