STINGRAYS AND TRIGGERFISH, PEN REGISTERS AND TRAP & TRACE: FOURTH AMENDMENT IMPLICATIONS OF RAPIDLY EVOLVING CELL PHONE SURVEILLANCE TECHNOLOGY

I. Definitions

A. Triggerfish and Stingrays

Triggerfish and stingrays are two models of a portable device that can detect signals emitted by a cellular telephone, including (1) the electronic serial number ("ESN") assigned to a particular cell phone, (2) the telephone itself, and (3) the telephone numbers called by the cell phone. When law enforcement uses triggerfish and stingray equipment, it is able to gather cell site data directly without the assistance of the service provider.

B. Pen Register and Trap & Trace

Historically, a pen register was a device that recorded the outgoing numbers dialed from a specific telephone number. Congress amended the definition in 2001 as part of the USA Patriot Act, and it is now defined as follows:

> The term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

18 U.S.C. § 3127(3).

The same statute defines a trap and trace device as follows:

> The term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

18 U.S.C. § 3127(4).

Congress also requires that a court order authorizing a pen register or a trap and trace device contain the following information:

> An order issued under this section--
>
> (1) shall specify--
>
> > (A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;
> >
> > (B) the identity, if known, of the person who is the subject of the criminal investigation;
> >
> > (C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and
> >
> > (D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and
>
> (2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

18 U.S.C.A. § 3123(b).

C. Why It Is Important to Distinguish Between These Devices

In 1979, the Supreme Court found that an individual has no reasonable expectation of privacy in the telephone numbers he or she dials. *Smith v. Maryland*, 442 U.S. 735, 743 (1979). Accordingly, the government has a low legal hurdle in applying for and receiving a pen register or track and trace device – instruments that merely gather incoming and outgoing telephone numbers. The government need only provide that information which the statute requires a court to include in its order authorizing a traditional pen register or trap and trace device.

When the government seeks signaling information to track an individual, however, the Fourth Amendment concerns increase. For instance, although an individual who is traveling on public streets in a vehicle has no expectation of privacy in his or her movements, *United States v. Knotts*, 460 U.S. 276 (1983), the government must obtain a warrant upon a showing of probable cause if it wishes to monitor a beeper in a private residence, *United States v. Karo*, 468 U.S. 705 (1984). Cell site location tracking allows the user to directly receive and send signals from and to a particular cell phone *without* the assistance of a service provider.

Triggerfish (which are also known as cell site simulators or digital analyzers), use the same technology as cell site location tracking: an antenna, an electronic signal processor, and a laptop to analyze the data.[1] Triggerfish imitate cell towers and have the ability to intercept a target cell phone's cell site data, which includes its telephone number, its electronic serial number, and the channel or codes identifying the location from which the cell phone is transmitting. If the phone is turned on, the triggerfish intercepts this data through "pings" approximately every seven seconds, as well as every time the phone initiates or receives a call and during calls. With this cell site data, triggerfish devices are able to track the location of the cell phone and determine the signal strength and direction of the intercepted frequencies. Triggerfish cannot, however, acquire historical cell site location information.

D. Fourth Amendment Concerns

The Fourth Amendment guarantees the right of citizens against unreasonable searches and seizures:

The right of the people to be secure in their persons, houses, papers, and effects,

[1] The Harris Corporation sells both the TriggerFish and the StingRay models, along with several other similar devices, which are cell site simulators or digital analyzers. The words triggerfish and stingray have become generic names, often used interchangeably, to refer to such devices. References herein to triggerfish are to all such models.

> 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.

U.S. Const. amend. IV.

The fundamental purpose of the Fourth Amendment is to "safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Camara v. Mun. Court of City & Cnty. of San Francisco*, 387 U.S. 523, 528 (1967). "As the text makes clear, 'the ultimate touchstone of the Fourth Amendment is reasonableness.'" *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)).

When the government applies for a pen register and/or trap and trace order, the statute requires that the government include in their application the target telephone number. In turn, the court's order must recite the target telephone number. When the government seeks to use a triggerfish device to detect signals emanating from unidentified cell phones within a specific vicinity, the court cannot issue an authorizing order under 18 U.S.C. § 1327 because no target telephone number exists. Instead, courts have determined that the government must seek a warrant for a triggerfish, which requires the government to make a showing of probable cause. Determining probable cause in a warrant requires the "judicial officer [to] decide 'whether, given all the circumstances set forth in the affidavit before him, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Warren*, 42 F.3d 647, 652 (D.C. Cir. 1994) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)).