F29 Spotting Stingrays: The Legal Issues of Covert Cell Phone Location Surveillance

Michael Buresh, JD, Cook County Public Defender, Chicago, IL 60602*

Learning Overview: The goal of this presentation is to introduce attendees to cell-site simulators, a covert cell phone location tracking device commonly referred to as a "stingray." The presentation aims to teach attorneys how to identify when a stingray has been used against their clients and how to seek legal recourse. This presentation will also cover the current state of search-and-seizure law on stingrays. Two real-life case examples in which law enforcement utilized stingrays will be presented to provide specific examples and to contextualize the presentation.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by explaining how attorneys can identify cases in which a stingray may have been used and how to uncover evidence of stingrays.

Cell phones communicate via stationary cellular antennae (cell sites, also commonly referred to as "cell towers") that relay phones' radio signals over long distances. Law enforcement can exploit this technology to conduct covert surveillance of citizens and their locations via a device called a cell-site simulator (a.k.a. "stingray"). Like "Kleenex®" or "iPad®," the term "stingray" derives from a specific brand of cell-site simulator manufactured by Harris Corporation. A stingray impersonates a real, carrier-operated cell site and forces all phones in the immediate vicinity to connect to it. The stingray then acts as a go-between, relaying signals between those target phones and the true, carrier-operated cell sites. These stingrays can decode these signals to reveal the identifying information of the phone (the International Mobile Equipment Identifier [IMEI]) and the identifying information of the customer (the International Mobile Subscriber Identifier [IMSI]). A stingray can act as a pen register/trap and trace device by intercepting all incoming and outgoing phone numbers to and from the target phone. A stingray also acts as a wiretap by intercepting the content of voice calls and text messages to and from the target phone. However, the most commonly used ability of a stingray is its ability to track the location of the target phone by measuring signal direction and strength. Stingrays can track multiple phones simultaneously and identify a specific individual's phone by the process of elimination.

As a covert surveillance device, law enforcement's use of these devices has been shrouded in mystery. Law enforcement agencies obtain these devices under strict Non-Disclosure Agreements (NDAs) with the Federal Bureau of Investigation (FBI). These NDAs prohibit local police from disclosing the existence or use of their stingray without the express permission of the FBI. The NDAs even commit local law enforcement to dismiss cases at the direction of the FBI if backed into a corner by a court. Police use vague language, parallel construction, legal fictions, and even outright lies to conceal their use of stingrays in criminal investigations.

The presentation will cover the current state of the law on stingrays. While there is no directly applicable United States Supreme Court opinion on the specific topic of stingrays, several lower courts and state legislatures have weighed in on the issue. This presentation will also cover two specific case examples in which clients of the presenter were "stung" and in which law enforcement went to great lengths to conceal their warrantless use of stingrays. In these cases, it was ultimately the work of independent government accountability and transparency activists (and their attorneys) that uncovered Chicago law enforcement's ownership and use of stingrays and secured justice for the clients.

Stingray, Cell Phone, Surveillance

*Presenting Author