F37 The Stingray® Revolution: How the Widespread Use of Cell Site Simulators Is Changing Law Enforcement Tactics and Criminal Prosecutions in Maryland

Jason D. Ricke, JD, LLM, Office of the Public Defender, 14735 Main Street, Ste 272B, Upper Marlboro, MD 20772*

After attending this presentation, attendees will understand how the use of a cell site simulator, known informally as Stingray®, is impacting criminal trial courts in Maryland and should be a concern for the greater forensic science community.

This presentation will impact the forensic science community by illustrating how the frequency of smart phone evidence in criminal cases makes the impact of its misuse substantial. Law enforcement agencies are using Stingray® as a forensic tool, oftentimes without court authorization, and attorneys and judges alike are scrambling to decide how to deal with this emerging technology.

As of early 2015, nearly 64% of American adults own a smart phone, a number that has nearly doubled from only 35% in 2011.[1] Smart phones contain call records, messages, location information, Global Positioning System (GPS) coordinates, audio/video, photographs, financial information, fingerprints, and even facial scans. The majority of these advancements in smart phone technology have become mainstream over the past five years.

The Supreme Court most recently recognized the importance of smart phones in Riley v. California.[2] The Court stated "modern cell phones are not just another modern convenience … with all they contain and all they reveal, they hold for many Americans 'the privacies of life.'"[3]

Nearly every defendant arrested for a crime is arrested with their smart phone. The evidence contained on these phones is a veritable gold mine of information that can be used in a myriad of ways by law enforcement and defense attorneys alike.

Law enforcement initially could gather information from the phone itself or from the phone companies, but now have new methods of obtaining smart phone evidence. One of the hot button issues is law enforcement's use of cell site simulators, known by the names Stingray® or Triggerfish.[4]

The forensic community should be concerned with any new technology being used to gather evidence with little to no oversight in criminal cases. The 2009 National Academy of Sciences (NAS) Report, Strengthening Forensic Science in the United States: A Path Forward, regarding the digital and multimedia discipline noted three challenges to digital evidence: (1) a lack of certifications/qualifications for forensic examiners; (2) agencies treating the examination of digital evidence as an investigative rather than forensic tool; and, (3) wide variability in the education, experience, and training of those practicing this discipline.[5] Stingray® presents problems for all three challenges. Some of the key topics are described below.

Current State of Technology and Future Developments: The Stingray® device used by many law enforcement agencies is manufactured and sold by Harris Corporation. The details surrounding its capabilities are carefully guarded. The Federal Communications Commission (FCC) filings for information on Stingray's® capabilities only reveal heavily redacted user manuals. Originally it was thought that the Stingray® device could only obtain a phone number, device ID, and location. It is now believed that Stingray® can read content from devices as well.[6] Once content can be pulled from the air, the lines between a virtual search and a physical search are completely blurred.

Impact of Technology on Law Enforcement: Local agencies in Maryland have confirmed using Stingray® since 2007. Due to non-disclosure agreements in place for the use of Stingray®, agencies do not discuss the use of Stingray® in their investigations. Maryland presents a unique environment in the use of this forensic tool given the proximity to many federal agencies tasked with protecting this technology. The agencies have used Stingray® in a collaborative effort with local enforcement that defer responsibility when questions do arise.

Emergence of Fourth Amendment Concerns and Discovery/Disclosure Methods: Attorneys in Maryland and across the country are scrambling to find answers. State agencies and the American Civil Liberties Union (ACLU) are filing public information act requests. Attorneys are using discovery requests and motions to suppress to ascertain when Stingray® is being used. The end result is that, rather than disclose the details of this technology to the public and the attorneys, the Federal Bureau of Investigation (FBI) has preferred prosecutors simply drop cases in which a cell site simulator was involved.[7]

The rapid expansion of smart phone technology combined with the new undisclosed methods of obtaining forensic evidence is changing criminal prosecutions in Maryland and across the country. Defense attorneys and prosecutors should be equally concerned because the use of a Stingray® device without proper oversight and disclosure leaves both sides getting stung.

*Presenting Author

Reference(s):

1. http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.
2. *Riley v. California*, 573 U.S. _____ (2014).
3. *Id*. At pg. 28.
4. https://www.aclu.org/map/stingray-tracking-devices-whos-got-them.
5. National Research Council, Committee on Identifying the Needs of the Forensic Sciences Community, *Strengthening Forensic Science in the United States: A Path Forward* (2009) at p. 181.
6. http://www.theguardian.com/us-news/2015/apr/10/stingray-spying-fbi-phone-dragnet-police.
7. http://arstechnica.com/tech-policy/2015/04/fbi-would-rather-prosecutors-drop-cases-than-disclose-stingray-details/.

Stingray, Jurisprudence, Digital Evidence