Forbidden Knowledge: Stingray cellular surveillance, DoJ antipathy for the Fourth Amendment, and the consequences of police militarization

Beau Hodai
DBA Press
July, 2014



Part 1: Introducing the fish

Harris Corporation, a Delaware corporation headquartered in Melbourne, Florida, is a true corporate behemoth-- reporting $5.11 billion in total revenue for 2013, with subsidiaries spanning the globe; from Afghanistan, Iraq and Qatar, to Romania, Russia, China, Chile, Papua New Guinea, the United Kingdom, and on.

Harris has its fingers in many pies-- from NASA communications systems to healthcare services-- though, arguably, the corporation's forte falls in the realm of defense/intelligence technologies.

Harris Government Communications Systems Division (Harris GCSD)-- a division which holds classified contracts with such defense intelligence heavies as the National Security Agency (NSA), and other intelligence agencies (not all of which are agencies of the United States)-- is home to Harris Wireless Products Group (Harris WPG).

Harris WPG produces a set of "cell site simulator" technologies used in interrogating data from and tracking cell phones.

Put simply, a cell site simulator is a device that impersonates the base stations (or "cell towers") of cellular service providers and forces cell phones within its area of operation to register and share information with it. Through this deception and forced registration, cell site simulator technologies interrogate phones for call data (who the phone has called, who has called the phone-- and the times and locations of such calls), device and cellular customer identifying data, registration data (i.e. what towers has the phone been in communication with, and at what times) and Global Positioning System (GPS) data. The contents of communications may also be intercepted through the use of these, and similar, technologies.

Cell site simulators have been in use by such agencies as the U.S. Department of Justice's (DoJ) Federal Bureau of Investigation (FBI) since at least the mid 1990's. However, in recent years-- thanks in large part to U.S. Department of Homeland Security (DHS) grant revenue streams available to local law enforcement agencies for the purported aims of "counter-terrorism," "emergency preparedness," or "all-hazards" mitigation, Harris WPG cell site simulators have experienced a renaissance of use in the domestic law enforcement/'intelligence' marketplace.

The most common set of Harris WPG cell site simulators that has been popping up in the hands of local law enforcement personnel nationwide has been some configuration of the following devices.

“Stingray:” according to Harris WPG documents, Stingray is a “transportable [cellular device] interrogation, tracking and location, and signal information collection system” that “performs network base station surveys, dialed number and registration collection, mobile interrogation, and target tracking and location.”

As stated in the Harris WPG documents, “[Stingray's] active interrogation capability emulates base station to collect MINS [Mobile Identification Number] and ESNs [Electronic Serial Number] through forced [customer cell phone] registration [with the Stingray cell site simulator].”

Stingray, and other Harris WPG products, may also be operated with a “PC interface” and Harris geolocation software that allows the operator to observe real-time geolocation data of phones within the device's area of operation.

[Note: the Harris WPG documents discussed in this section are Harris WPG law enforcement sales brochures, not intended for distribution outside of law enforcement/intelligence circles. The documents cite Title 18 of the U.S. Code, Section 2512, pertaining to criminal restrictions on the publication of advertising materials for communications intercept devices. Under 18 USC 2512, such advertisements may only be published, transmitted or possessed by lawful communications industry manufacturers of such devices and government employees/government contractors.

The documents are referenced by *DBA Press* as they appear in the federal court record court record of litigation between Daniel David Rigmaiden and the Federal Bureau of Investigation (FBI) concerning Freedom of Information Act (FOIA) requests filed by Rigmaiden with the FBI seeking records pertaining to these technologies and other related issues.]

“Stingray II:” while the exact distinction between Stingray and Stingray II is not known, photographs of the device suggest that Stingray II is capable of simultaneously operating multiple channels on multiple networks, using multiple direction finding and GPS antennae.

“Kingfish:” as described in Harris WPG documents, Kingfish is a “portable [cellular device] interrogation, direction-finding, and collection system” that “provides investigators with a tool that extracts the telephone number (MIN) and Electronic Serial Number (ESN) from a [...] mobile telephone. The active direction-finding (DF) capability enables location of a powered-on phone without depending on the suspect to be involved on a call. Additionally, Kingfish provides passive dialed number recorder (DNR) and registration collection capabilities. Passive operations identify calling patterns and provide information on the suspect's area of operation.” The system also “provides [a] real-time display of interrogation and passive collection results.”

“Amberjack:” according to Harris WPG documents, Amberjack is a “direction finding antenna system capable of tracking and locating mobile phone users and base stations,” designed for use with Stingray, Stingray II, Kingfish and a number of other Harris WPG cell site simulator-based technologies.

The antenna resembles a large frisbee (17 inches by 4.2 inches, weighing in at 14 pounds) and is outfitted with magnetic mounts for ease of placement on tracking vehicles.

“Harpoon:” according to Harris WPG documents, Harpoon is a “high-power filtered amplifier that

maximizes the multichannel transmit capability of the Stingray II and significantly improves the performance of the single-channel Stingray and Kingfish systems." The amplifier is capable of boosting the total output power of these devices up to 30 watts per band, significantly increasing the area of interrogation/tracking.

"Hailstorm:" this device began appearing in local law enforcement procurement documents in early 2013, generally as an "upgrade" to Stingray II. According to a March, 2014 Harris Corporation General Services Administration (GSA) price list, Hailstorm is also available as an upgrade to Kingfish and Stingray. Hailstorm is available as a standalone product as well.

Very little is known about Hailstorm, aside from the fact that this technology costs agencies approximately $65,000 to $330,000 (the lower end of this price spectrum applies to purchases of Hailstorm upgrades to existing technology), that it stands on the shoulders of Stingray II and Kingfish cell site simulators, and that purchases of Hailstorm also are commonly accompanied by amplifier upgrades and new "cellular utilization" software purchases.

According to procurement documents, Hailstorm is also compatible with hardware manufactured by another contractor that allows for "close quarter and foot tracking [of suspects]"-- though this "foot tracking" ability does not appear to be a feature exclusive to Hailstorm, as Stingray systems and Kingfish appear to have similar capabilities.

A number of other Harris WPG accessory technologies to this core set of cell site simulators allow their users to intercept the contents of cellular communications and block/disrupt cellular use.

Accessorize your fish: supplemental surveillance resources

Pen-Link, a Lincoln, Nebraska-based producer of law enforcement Communications Assistance for Law Enforcement Act (CALEA)-based intercept/surveillance software and hardware products, produces a number of products that Harris Corporation (according to procurement documents) recommends for use with their cell site simulators Stingray, Stingray II, Hailstorm, and, very likely, Kingfish. However, Harris cell site simulators and Pen-Link equipment are not mutually dependent; these are stand alone products that are often used in conjunction with each other to form a powerful intelligence gathering and analysis system.

CALEA, as passed in 1994, in response to a direct congressional request from the FBI, essentially mandated that all telecommunications carriers in the United States ensure that their networks be open to, and compatible with, law enforcement communications surveillance/interception techniques. In 2006, the Federal Communications Commission (FCC) issued further orders based on CALEA, requiring that "facilities-based broadband internet access providers" (as opposed to wireless internet providers-- already covered under CALEA 1994) and Voice Over Internet Protocol (VOIP) service providers (such as Skype) come into compliance with CALEA.

Under CALEA, communications carriers are required to provide law enforcement (having obtained appropriate court orders, or citing "exigent circumstances") with ongoing, recent or historical communications content (CALEA-compliant carriers must be able to provide government agencies with communications "concurrently with their transmission," or "at such later time as may be acceptable to the government"), as well as non-communications-content "communications identifying

information" (such as dialed and received numbers/internet protocol addresses, dates/times of communications, et cetera). Under CALEA, carriers must be able to provide this information electronically, in formats decipherable to law enforcement agencies.

As such, some law enforcement agencies believe that the are entitled, through CALEA, to a direct line of all cellular customer data, and that Pen-Link is, as it describes itself, the key to the kingdom (Pen-Link's registered trade mark slogan is "[Pen-Link]It's the Key").

As stated by the Tennessee Bureau of Investigation in a September, 2013 Pen-Link wiretap system purchase memorandum: "[CALEA] requires telecommunications providers to have a means to deliver call data directly to law enforcement computers [...] Law Enforcement must have compatible technology in order to be able to make use of this service." And, as stated by the Oakland County (Michigan) Sheriff's Office in an April, 2013 Harris Hailstorm/Pen-Link software purchase order: "[Pen-Link software] connects the Hailstorm equipment to all cellular phone companies through a direct internet connection."

Pen-Link equipment (which often includes both software packages and dedicated Pen-Link servers/computers-- presumably needed for the massive amounts of data storage entailed by Pen-Link use), used in conjunction with Harris WPG cell site simulator technologies, essentially allows law enforcement officers to apply both geolocation (either GPS or cellular base station registration) data and other cellular customer call data (i.e. logs of calls and callers, including base station registration data associated with these calls) to multiple matrices of data-- including CALEA cellular service provider data.

For example, according to Pen-Link Territory Sales Manager Shelley Sorensen (procurement records show that Sorensen has been the PenLink representative in a number of Florida law enforcement Pen-Link purchases, so her "territory" is likely the southeast portion of the nation), it is often vitally important for officers employing cell site simulators in tracking cell phone users to be able to place their subject phone within a certain geographical area prior to the deployment of a cell site simulator.

This is done, according to Sorensen, with cellular customer data "streamed down" to Pen-Link from cell service providers.

"[Stingray] is used to go out and kind of ping cell phones-- so you can find out where, you know, your bad guys are. What it does is it kinda acts as almost a cell tower for that cell phone-- and then you're able to determine exactly where they're at. But, the thing with that is you can't just drive it up the driveway and expect it to go find that phone, okay-- it has to be within a proximity," said Sorensen. "And that's where the Pen-Link software comes in, because you can do real-time pen registers, is what they're called. A pen register is, ah, like a wiretap without the audio, basically. But, you get, you know, the date, time, duration [of calls], the number they're calling-- all that kind of stuff. But, you also get the cell tower that they're hitting off of-- so, as soon as they get off that cell tower on your pen register, which Pen-Link is gonna show you, then you know 'okay, here's where we need to take the truck, because we know they're hitting off of this tower."

"Even when you get the Stingray, it has its own set of software," said Sorensen, speaking to the capabilities "Stingray" ["Stingray" in this case may be used generically to refer to multiple Harris WPG cell site simulator technologies] operating sans Pen-Link CALEA assistance. "Because, then you

pull that up, and that thing, once you're in a location, that software actually kinda-- it's almost like a cat-and-mouse kind of game. If you're going down the right street, it's gonna give you a stronger meter of you're gettin' closer. Um, kind of, when I've seen it, the guys kind of know that, 'oh, you know, his girlfriend lives around here, so I bet that's where he's at'-- so that's usually how it goes. But, yeah, I think that that piece of software is kind of, 'okay, we're in the region now, we're gettin' close' and the meter's kinda tell you if you're goin' the right direction tryin' to find that guy."

It should be noted here that neither Harris WPG cell site simulators or Pen-Link equipment are limited to telephonic cellular use.

In 2008 Daniel David Rigmaiden, sought for a large scale IRS fraud conspiracy (Rigmaiden assumed the identities of dead taxpayers and filed millions of dollars worth of false tax returns using IRS "e-file" programs) was arrested after his Verizon cellular internet Aircard was located through the use of Stingray cell site location-- in a very similar manner to that described by Sorensen in reference to joint Stingray and CALEA data use.

And, according to Pen-Link documents, their equipment is compatible with such technologies as the DCS 3000 internet communications intercept/"packet sniffer." The DCS 1000 "Carnivore" was a technology developed for use by the FBI that intercepts internet data packets, which are the internet traffic equivalent to telephonic "communications identifying information"-- such as email to/from data and data pertaining to IP address internet traffic.

According to a 2006 Department of Justice Office of the Inspector General CALEA implementation report, the DCS 3000 "is an interim solution [alternately referred to as an "ad hoc" solution implemented in order to address then-CALEA compliance shortfalls] to intercept personal communications services delivered via emerging digital wireless technologies used by wireless carriers [...]."

Pen-Link is also compatible with such commercially produced cellular/internet communications intercept/"packet sniffer" devices as the Verint Reliant. Verint Systems, Inc. produces such technologies largely for consumption by state/regional 'fusion centers,' which are funded in large part through DHS grant streams.

But, this is only the entrance point for the manifold potentials presented through the combination of Harris cell site simulators and Pen-Link equipment.

Pen-Link equipment essentially serves as an automated intelligence analyst; when used in conjunction with Harris WPG products, the system can integrate both real-time (tracking data obtained while targets-- or every phone in an area of coverage-- are on the move) and historical data (such as cell customer dialed/received numbers and base station registration) gathered through the use of Harris WPG cell site simulators and/or the CALEA-compelled assistance of carriers, and integrate these data sets with data sets provided through the "national intelligence" databases of other government agencies (such as FBI, Immigrations and Custom Enforcement, and the U.S. Marshals Service), as well as privately-held collections of civilian data and cellular customer data (such as those maintained by Reed Elsevier/LexisNexis/Choicepoint NeuStar and Pen-Link itself).

Given the fact that much of this cellular customer data used in conjunction with the Harris WPG cell

site simulators is contained in private databases held by either Pen-Link or its partners, it appears that the Pen-Link system can be used quite effectively without the assistance of cellular service providers, and court orders that would be required for such assistance (baring, of course, those circumstances in which law enforcement seek CALEA data citing 'exigency').

The end results may include graphing of interpersonal relationships (based largely on frequency of calls to an from numbers, as well as cell site registration information. Such techniques may also be used to identify the users of pre-paid “burner” phones. Such intelligence gathering tasks may be performed by Stingray with the CALEA facilitation and analytical capabilities of systems such as Pen-Link, or by Stingray systems independently) and personal travel histories that can reveal both the paths of travel used by cellular customers, as well as habitual daily movement routines (these graphs would be largely based on cellular registration data-- potentially composited through the use of Harris WPG cell site simulator interrogation of phones and cell towers, as well as through CALEA-compelled carrier information and/or other databases).

With such abilities at the fingertips of local cops as would make the Stasi stand up and spontaneously ejaculate, what more could Hailstorm offer? According to Sorensen, not even Pen-Link knows.

“I'm not sure about the Hailstorm.... I'm not... that.... that.... you asked me a question that I just don't know the answer to [...] I thought I was doing so well,” said Sorensen, who went on to say that there is no one at PenLink who deals with the Hailstorm system specifically. “You'd have to hit up those guys at [Harris], 'cause they're pretty-- and for a good reason-- but they're pretty, um, noncommittal to talking about stuff to anybody who's not law enforcement or military.”

[For more on such automated analytical systems, and how those systems are applied to such “open source intelligence” as social media, see “Inside the OpenMind” (http://dbapress.com/archives/3476) and “Dissent or Terror” (http://dbapress.com/archives/3121)]

With great power comes great corruption

There is one more concept to consider where the marriage of the raw data gathering power of Harris WPG cell site simulators and Pen-Link (or similar) analytical resources are concerned: when used in conjunction with a Stingray, Kingfish, or Hailstorm device, Pen-Link (or other analytical products, potentially including the Harris WPG “PC Interface”) stores the data obtained by the cell site simulators for analysis. There is also evidence to suggest that Harris WPG devices may independently store such data.

In order to facilitate these-- and other-- analytical functions, Pen-Link units serve as mass data storage units (which are linked, in turn, with other mass databases). While, according to Sorensen, Pen-Link is intended to store and analyze only data pertaining to those phones that are specifically targeted by court orders, the Harris products-- by their very nature-- gather data from every single cellular device in their area of operation (or, in the case of cellular base station interrogation, they gather data on every single phone that has registered with individual tower during a specific period of time).

It is also important to note that not all instances of Harris WPG cell site simulator use incorporate Pen-Link, or other non-Harris analytical systems; Harris systems do work with their own PC interfaces and do have features expressly intended for the recording and storage of gathered data, as well as for the

production of surveillance intelligence products (such as those that might be submitted in the course of a prosecution as evidence).

What may happen with this data-- gathered en masse from "innocent" phones (and, to be sure, the FBI has confirmed, through an affidavit submitted in the Rigmaiden case, that such "innocent" cellular data is intercepted by these devices)-- is a matter of grave concern for critics of such systems, especially when some agencies seem to hold extremely cavalier attitudes regarding the warrantless collection of data from citizens exercising no more of a predicate of criminal activity than attendance at a protest.

For example, as stated in a November, 2003 retroactive "emergency purchase" authorization document allowing the Miami-Dade Police Department (MDPD) to purchase a Stingray and Amberjack, police needed the devices in order to surviel protestors. In fact, police felt such exigency was present in this situation that MDPD had spent $115,500 on the purchase of these systems without authorization-- later seeking retroactive retroactive authorization. As stated in the retroactive authorization document:

"[In order to provide] the level of security commensurate with the [Free Trade Area of the Americas, "FTAA"] Conference, it was necessary to enter into this emergency purchase. [...] Based on the history of these conferences, the department anticipated criminal activities directed at attendees and conference sites facilitated by the use of cellular phones. Wireless phone tracking systems utilized by law enforcement have proven to be an invaluable tool in both the prevention of these offenses and the apprehension of individuals attempting to carry out criminal activities.

"MDPD already possessed wireless tracking capability via the Harris Corporation's Triggerfish tracking system. that system was limited in that it provided access to only Cingular and AT&T Wireless carriers. The newly developed Sting Ray/Amberjack [sic] system by Harris Corp. provides PCS tracking capability, which includes Metro PCS, Sprint and Verizon carriers. The combination of these two tracking systems, Triggerfish and Stingray/Amberjack provided MDPD the ability to track approximately ninety percent of the wireless industry."

The 2003 Miami FTAA conference was marred by allegations of heavy-handed police tactics against protestors, including: the special use of municipal ordinances to restrict protest activity, the use of heavily armed and armored mobile field force units, unjustified personal searches, mass arrests and police brutality-- all of which would become hallmarks of police reactions to protests, particularly during subsequent Democratic National Committee and Republican National Committee presidential conventions, and-- most notably-- during the widespread Occupy Wall Street protests of 2011 and 2012.

[For more on the use of DHS-funded surveillance programs and their application to citizens engaged in free speech and activism, see "Dissent or Terror" (http://dbapress.com/archives/3121)]

[Note on moving forward: the specific Harris WPG product names of some devices subsequently discussed are not known. As such, in some cases, *DBA Press* generically refers to Harris WPG cell site simulators simply as "Stingrays," "Stingray systems," or some variation thereof.]

An example of Stingray in use

According to a transcript in a Second Judicial District of Florida case (*Florida v. James Thomas*), in

September of 2008, Tallahassee Police Department (Tallahassee PD) officers located and arrested Thomas, who was being sought under suspicion of sexual assault and theft, using a Stingray device. The transcript, describing the circumstances of Thomas' arrest, provides a rare glimpse into the methods of law enforcement officers employing a Stingray system ["Stingray" is used as a generic term for Harris WPG cell site simulators in this section, as the exact device used in this instance is not known].

The referenced transcript (of a suppression motion hearing that took place on August 23, 2010) had remained under seal due to the disclosure of Stingray use contained therein. The transcript was unsealed on June 2, following a successful motion to unseal filed and argued by the American Civil Liberties Union (ACLU) of Florida.

According to the testimony of Tallahassee PD Technical Operations Unit Investigator Christopher Corbitt, immediately following Thomas' commission of the sexual assault, the victim reported the assault to Tallahassee PD, and informed officers that a number of her belongs had been taken from her by Thomas-- including her cell phone.

A group of Technical Operations Unit officers under the command of Corbitt then began a hunt for the phone-- the logic being that if they found the phone, they would find Thomas.

Corbitt and his men obtained the phone's MIN and ESN from Verizon (per CALEA), as well as information indicating what tower the phone was currently registered with. Using this basic geographical location, Corbitt and is men then struck out in a vehicle outfitted with a Stingray device. The ensuing location process entailed a period of several hours wherein the officers drove around this basic geographic area, interrogating cellular devices contained both in public areas and within private property (such as residences and businesses), searching for the presence of their target phone.

Describing this investigative process, Corbitt divulged a few interesting aspects of Stingray use. For instance, as stated by Corbitt, the device is only able to interrogate and/or track devices that are powered on.

And, as stated by Corbitt, during its interception and forced registration of cellular devices, the Stingray device causes cellular devices in its area of operation to broadcast their signals to it at maximum power. As such, cell phones within an area of Stingray use drain their batteries more rapidly than they would normally.

This fact-- the decreased lifespan of the victim's cell phone due to Stingray use, as well as the natural limitation of cell phone battery life-- was alluded to in Corbitt's testimony as having been a factor of exigency in Tallahassee PD's location of Thomas, and subsequent debate as to whether a search warrant should be obtained once Thomas' location was determined.

This exigency inherent to Stingray use in cell phone tracking may provide a built in "exigent circumstance" exemption to court order requirements for CALEA-mandated carrier assistance. According to records obtained by *DBA Press*, Tucson Police Department (TPD) officers cited exigent circumstances in obtaining "phone activity and recent cell tower activations" from Cricket Communications during their use use of a Stingray system in an attempt to locate a cell phone belonging to a missing person in September of 2012. According to TPD records, there was no

indication of foul play, nor was there any indication that the individual being sought had come to any harm; the missing person simply hadn't been seen since leaving for work a day prior. The only apparent grounds for “exigency” in this case would have been cellular battery life and/or diminishment of battery life through the use of the Stingray device. Outside of the exigent request issued to Cricket Communications by TPD in this case, no court order was sought for the purpose of obtaining this customer data.

Eventually, Corbitt and his men honed in on the Berkshire Manor apartment building.

Having located the apartment complex the stolen phone was likely in, Corbitt “went home for a little bit,” then recommenced the work of locating Thomas shortly after midnight.

According to Corbitt, he and his officers then took a handheld cell site simulator unit and “quite literally stood in front of every door and window” in the Berkshire Manor apartment complex in order to “measure the direction of where the signal was emanating from.”

Eventually, at approximately two o'clock on the morning of September 14, 2008, this process led officers to apartment 251, where the stolen phone was located and where Thomas was arrested.

It is important to note here that the Stingray is an “active,” as opposed to a “passive” surveillance device-- which means that Stingrays, rather than sitting idly by and waiting for data to swim into their mouths, actively seek out and intercept data. This, of course, is done by transmitting a signal that mimics that of a cell tower, forcing responding phones to register with it, and then interrogating those responding phones. So, given this fact, Corbitt is describing a process through which his men actively searched the contents of every single apartment unit in the Berkshire Manor complex, (and seized whatever data phones may have been forced to share during their forced registration with the officers' Stingray device) by standing outside of each and every door and window in the apartment building while transmitting these false and interrogatory cell site signals into the homes of people who had nothing to do with their investigation.

As stated by Corbitt in the hearing transcript, this search of the entire Berkshire Manor apartment complex (conducted without a search warrant) was executed in order to find probable cause for the physical search of one apartment. This is a vital point: the testimony of Corbitt contained in the suppression hearing transcript clearly states that officers committed what is arguably an unconstitutional general search of an entire apartment building in order to find probable cause to serve as the legal basis for a search of one single apartment.

Despite the fact that officers had established probable cause for the search of apartment 251 through the use of Stingray, in the end the Tallahassee PD officers opted to enter and search without a warrant.

“I know there was discussion about a search warrant. I had indicated to the investigators that I believed probable cause existed to say that property belonging to the victim was within that apartment and was wiling to complete an affidavit for a search warrant,” said Corbitt under examination of Thomas Defense Attorney Daren Shippy. “And that was eventually determined, that a search warrant was not necessary based on other factors [...] As always, we prefer that alternate legal methods be used, so that we do not have to rely upon the equipment to establish the probable cause, just for not wanting to reveal the nature and methods.”

Corbitt went on to state that the Tallahassee Police Department had never obtained a warrant to search a location "based solely on the equipment," largely due to the "proprietary" nature of the equipment, as well as a desire on the part of Tallahassee PD to keep the capabilities of the system a secret-- even if that meant concealing evidence gathered through such investigative methods from defendants and their counsel.

Speaking to concerns arising from the "proprietary" nature of the Stingray system, earlier in the hearing Assistant State Attorney Kathryn Ray advised the court that the Tallahassee Police Department was subject to a non-disclosure agreement concerning the use of the Stingray system.

According to ACLU Speech, Privacy and Technology Project Staff Attorney Nathan Wessler, the Tallahassee PD preference toward "parallel construction" (a practice wherein some alternate legal grounds for search and seizure under the Fourth Amendment are cited in place of actual, often legally-questionable, methods used) in the Thomas case is a troubling indication that officers using Stingray technology may be deliberately avoiding judicial disclosure and oversight of Stingray technologies.

Part 2: Introducing the law-- the Fourth Amendment versus the Third Party Doctrine

The Fourth Amendment of the Constitution of the United States establishes:

"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."

Critics of domestic law enforcement use of cell site simulators argue that the devices' operation constitutes both search and seizure of personal data (i.e. "papers") from personal "effects" (i.e. personal cellular devices), in that, when a Stingray is in use, law enforcement officers are transmitting signals into the personal devices of individuals (including during times when those devices are located in the private residences of their owners) for the purpose of interrogating (searching for) and seizing data from those devices.

Furthermore, critics argue that Stingray-- a device that, integral to its operation, interrogates and seizes data indiscriminately from every phone within its area of operation-- constitutes a direct violation of Fourth Amendment protections from unreasonable search and seizure, in that such search and seizure is not backed by probable cause, and is not limited in scope pertaining to what specifically is to be searched/seized or where such search/seizure is to occur (as such searches under a search warrant are).

This speaks to the larger question of whether cell site simulator use in its current form is legal at all.

"There is a much more fundamental question about whether IMSI catchers [International Mobile Subscriber Identity; 'IMSI catcher' is another term used to describe cell site simulators] can ever be used constitutionally, under the Fourth Amendment," said ACLU of Northern California Staff Attorney Linda Lye.

"My colleagues and I have serious doubts as to that because an IMSI catcher, by its very operation, is

incredibly indiscriminate. It scoops up the information, not just of the target device, but all devices in the proximity. So, it engages in the electronic equivalent of the general searches that are prohibited by the Fourth Amendment.

“The framers adopted the Fourth Amendment [...] in reaction against the British practice of engaging in general searches. Under the rubric of these so-called 'writs of assistance,' the British used to search wherever and whatever they pleased to look for violations of the British customs laws. The framers adopted the Fourth Amendment in reaction to that practice, and specifically adopted something called the 'particularity clause' in the Fourth Amendment, which requires the government to specify the places or persons to be searched, so things could be seized-- with particularity-- and to make clear that the government can only search those things as to which there is probable cause.

“You can't just search a one-hundred-unit apartment building-- every single unit-- because you think the suspect might be living in one of those units, but you don't know which one. That's exactly what a Stingray does-- it searches everything, to find the one thing.”

According to Federal Communications Commission (FCC) records pertaining to Harris Corporation's authorized production and distribution of cell site simulator technologies, Harris has requested a number of provisions on the use of these products. Chief among these provisions are requirements that Harris Stingray systems only be domestically available for use by federal, state and local public safety/law enforcement agencies-- and that “state and local law enforcement agencies must advance coordinate with the FBI the acquisition and use of equipment authorized under this authorization.”

The U.S. Department of Justice (DoJ), the FBI's parent agency, has long held that, generally, the appropriate judicial authorization for the use of Stingray devices are court orders for the use of “pen registers” and “trap and trace” devices.

Under federal law [18 USC, Chapter 206 (sections 3121 through 3127)], a pen register is defined as:

“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 [...]”

Under federal law, a trap and trace device is defined as:

“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.”

As such, pen registers and trap and trace devices form two sides of the non-communications content coin, as tandem use obtains both information dialed by a customer's phone, as well as information pertaining to those who dial the number belonging to the subject of investigation. Court orders authorizing the use of these devices are often sought in tandem. [Pen register/trap and trace orders are collectively referred to as “pen/trap orders” throughout.]

The U.S. Supreme Court's 1979 ruling in *[Michael Lee] Smith v. Maryland* has been used to assert a

'third party doctrine' where such phone records (and, subsequently, internet records) sought through the use of pen registers and trap and trace devices are concerned. While the acquisition of phone customer data may seem like a search and seizure of personal effects (and therefore subject to protections under the Fourth Amendment to the U.S. Constitution), the High Court stated that, due to the fact that such personal information is entrusted and transmitted by the customer to, and through, the service provider (the third party), the customer has no reasonable expectation to privacy, nor do they have any reasonable expectation that this information in the possession of such a third party should be secured from law enforcement under the Fourth Amendment.

It is this perceived exception of such data from Fourth Amendment protections against unreasonable search and seizure that has proven to be such a boon for law enforcement officers seeking to surveil citizens through the use of cell site simulators; where a much higher burden-- that of probable cause-- is demanded by courts for the issuance of search warrants, a much lower standard is held for obtaining court orders for the use of pen registers and/or trap and trace devices. This much lower standard applies at both the federal and state levels, with many states emulating, if not mimicking precisely, federal pen/trap law.

For example, under federal law a court is compelled to grant a requesting officer a pen/trap order if the officer “has certified to the court that the information *likely* to be obtained by such installation and use is *relevant* to an ongoing criminal investigation” [emphasis added]. Note the lack of any probable cause requirement; any requirement of an explanation of the nature of the investigation in question; any disclosure of technologies to be used, or their capabilities outside the legal definition of pen/trap devices; or even any burden of demonstrating that a criminal offense has actually been committed.

While the requirements of pen/trap orders fall well below the bar of criteria necessary for the acquisition of search warrants, these lax criteria are often too burdensome still for law enforcement officers seeking to use cell site simulators in tracking/surveillance.

In many cases, law enforcement officers opt to claim “exigent circumstance” exemptions to pen/trap statutory requirements.

Or, as previously discussed, through a practice known as “parallel construction,” law enforcement officers simply employ their cell site simulator without telling anyone (including judges), and then later cite some alternate "legal method" (to borrow Tallahassee PD Investigator Corbitt's phrasing) or source as being the origin of information gained through the use of the cell site simulator.

An example of parallel construction may be as follows: police determine the location of a suspect within a residence through Stingray use. Officers raid the location, seeking the suspect. Rather than divulging this Stingray use, the officers report that they had received an 'anonymous phone tip' pertaining to the suspect's whereabouts. Coupled with some claim of exigency (i.e. an officer claims that a woman was heard screaming inside the residence), a warrantless search becomes 'a good faith effort on the part of officers acting on a tip from an anonymous citizen, bolstered by the urgency of the woman's screams within the residence.'

Remember this rhetorical example of "parallel construction," as it is not so rhetorical and will be discussed in much greater detail shortly.

DoJ notion of Stingray outside the Fourth Amendment Standing on Shaky Ground

Regardless of DoJ's stance that Stingray use falls outside of the protections of the Fourth Amendment, there has been some dissent in the federal court system-- calling into question whether this stance would hold if law enforcement were to disclose the nature of this technology to judges when seeking pen/trap, or other, orders.

In 1995, an assistant United States attorney (AUSA) acting on behalf of the Orange County Regional Narcotics Suppression Program approached U.S. District Court for the Central District of California Magistrate Elgin C. Edwards and requested a pen/trap order for the use of a "digital analyzer" (it is not known what, if any, differences in capabilities there may have been between this device and present day cell site simulators).

Ultimately, Edwards did not grant the order for two primary reasons:

At the time of the request, federal pen/trap statute was not viewed as applying to cell site simulators because the letter of the law at that time defined "pen register" (and, similarly, trap and trace devices) as being a device "which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line *to which such device is attached* ..." [emphasis and ellipses contained in Edwards opinion, not in statute].

As such, one of the reasons Edwards did not grant the pen/trap order request was that pen/trap statute did not apply to cell site simulators in 1995, as statue described devices attached to physical telephone lines. Language in the statute was later modernized through the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" ("USA PATRIOT ACT of 2001").

The second primary reason Edwards denied the pen/trap order is a little more interesting in that it applies to the reality of cell site simulators today-- namely, the collateral interception of data from phones not targeted by the order, combined with an inherent absence of accountability should law enforcement be permitted such free rein.

As stated in the Edwards denial:

"The order sought [...] would not insure sufficient accountability. For example, depending upon the effective range of the digital analyzer, telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted. Also, it may be that individual subjects of the investigation use a plurality of cellular phones having different numbers [the application did not identify any specific numbers to be surveilled]. With the present order sought by applicant, all such telephones could be analyzed without any record being produced."

In June of 2012, Magistrate Judge for the U.S. District Court for the Southern District of Texas, Corpus Christi Division, Brian Owsley issued an opinion on an AUSA request for Drug Enforcement Agency (DEA, an entity of DoJ) authorization for use of a Stingray device under a pen/trap order. Owsley had rejected the application and the resultant opinion is the most probing piece of judicial skepticism

offered to date pertaining to the DoJ notion that cell site simulators operate outside of Fourth Amendment protections.

The AUSA and a DEA agent had approached Owsley with the application and stated that a subject of an ongoing investigation had gotten a new phone with an unknown phone number, and that they would like a pen/trap order for the use of a Stingray.

The Stingray, as stated in Owsley's iteration of the application, would "'detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones (e.g., by transmitting the telephone's serial number and phone number) to the network for authentication.' The applicant further explains that "[b]y determining the identifying registration data at various locations in which the [Subject's] Telephone is reasonably believed to be operating, the telephone number corresponding to the [Subject's] Telephone can be identified.'"

In his opinion, Owsley observed:

"The application has a number of shortcomings. It does not explain the technology, or the process by which the technology will be used to engage in the electronic surveillance to gather the Subject's cell phone number. For example, there was no discussion as to how many distinct surveillance sites they intended to use, or how long they intended to operate the stingray equipment to gather all telephone numbers in the immediate area. It was not explained how close they intend to be to the Subject before using the stingray equipment. They did not address what the government would do with the cell phone numbers and other information concerning seemingly innocent cell phone users whose information was recorded by the equipment.

"While these various issues were discussed at the hearing, the government did not have specific answers to these questions. Moreover, neither the special agent nor the [AUSA] appeared to understand the technology very well. At a minimum, they seemed to have some discomfort in trying to explain it."

Furthermore, as observed by Owsley, the proposed practice of using a cell site simulator in order to capture the identifying information of every single phone in any given area chosen by law enforcement, at any given time chosen by law enforcement, in order to obtain one unknown telephone number was at odds with statutory requirements for the application for pen/trap orders, as applicants are required to be able to identify the phone number or other identifier of the target phone/device.

And, as the AUSA and DEA sought the use of Stingray under a pen/trap order for the purpose of collecting the identifying information of unidentified phones themselves-- as opposed to phone numbers dialed or associated with incoming communications to/from specific known target phones (as pen/trap devices are defined by statute)-- Owsley determined that a search warrant under the Fourth Amendment would be appropriate authorization, not a pen/trap order.

Aside from these instances of judicial eyebrow-lifting, DoJ has good reason for wanting to shield the capabilities of Stingray systems from the eyes of judges. Setting aside the fact that Stingray use may well constitute general searches prohibited by the Fourth Amendment, there have been a number of rulings indicating that the judiciary would place Stingray well within the realm of the Fourth Amendment-- and all of the burdens of probable cause and limitations of search and seizure imposed by it-- if the judiciary were more fully informed as to Stingray's methods of operation.

In the Rigmaiden case, the federal government chose to concede, rather than produce discovery materials sought by Rigmaiden pertaining to Stingray, that their use of the Stingray system amounted to a deployment of invasive technologies used in a search (of a private "effect"-- i.e. Rigmaiden's Verizon Aircard) and seizure (of "papers"-- i.e. data contained on Rigmaiden's Aircard) under the purview of the Fourth Amendment. This admission did not go unnoticed by Owsley, who cited it in his opinion regarding Fourth Amendment applicability to cell site simulators.

In 2001 the U.S. Supreme Court ruled, in *[Danny Lee] Kyllo v. United States*, that the invasive use of thermal imaging equipment in searching personal property was an action subject to the Fourth Amendment, and therefore required probable cause and a search warrant.

Kyllo had been arrested in 1992 on charges of growing marijuana following a thermal imaging scan (sans warrant) of his home.

It certainly could be argued that the transmission of cell site simulator signals into private homes in order to search out and seize data, as conceded to in the Rigmaiden case, may well constitute the same set of issues as was ruled on by the High Court in *Kyllo*.

In 2012 the U.S. Supreme Court ruled, in *United States v. [Antoine] Jones*, that the use of GPS tracking devices placed on the vehicles of surveillance subjects constitutes a "search" of "private effects" for which there is an expectation of privacy (i.e. a vehicle and/or any private area where that vehicle is stored). As such, the High Court held that this form of tracking/surveillance activity constitutes an action subject to protections under the Fourth Amendment.

On June 11 of this year, a judge in the United States Court of Appeals for the Eleventh Judicial Circuit ruled, in *United States v. [Quartavious] Davis*, that the government must obtain a search warrant for the collection of cellular customer cell site registration/location records.

In 2011 a grand jury for the U.S. District Court of the Southern District of Florida returned an indictment against Davis, alleging a role in a string of armed robberies. During Davis' trial, the government produced cellular registration/location records that showed Davis and accomplices made and received several calls in locations coinciding with he locations and times of the robberies.

In the Davis case agents had used court orders similar to pen/trap orders. This order, issued under the Stored Communications Act (18 USC 2703 (d)), requires a threshold of disclosure approximating that required in the application for a pen/trap order:

"[courts shall issue an order] if the governmental entity offers 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."

Orders under 18 USC 2703 (d) are generally referred to as "hybrid orders," and DoJ has, at times, held that such orders suffice as authorization for the use of Stingray devices in cellular device tracking using base station registration data.

The June 11 opinion only influences courts within the Eleventh Judicial Circuit, however. The Eleventh

Judicial Circuit hears appeals from federal courts in Alabama, Georgia and Florida.

On the June 25 U.S. Supreme Court ruled, in *[David Leon] Riley v. California*, that law enforcement searches of cell phones constitute to a Fourth Amendment search, and therefore require a search warrant-- except in cases of "exigent circumstances."

The impact, if any, of these recent court rulings on DoJ's cell site simulator guidance is not yet known.

Part 3: Having their cake and eating it too-- a dramatic instance of DoJ dedication to Stingray secrecy and the convenient blurring of lines between federal and local jurisdictions

Louise Goldsberry is an operating room nurse employed at Doctors Hospital in Sarasota, Florida. On the evening of Wednesday, July 17, 2013, Goldsberry was at home in her Hidden Lake Village condo, spending some time with her boyfriend, Craig Dorris.

"I was washing dishes after a long day in the OR and I even had a glass of wine, my boyfriend was over-- and I looked up from my kitchen window, into the barrel of an assault rifle carried by a man that looked like, I don't know, Rambo-- khaki stuff, like a hunter's kind of vest, [...] I was shocked. I thought it was a home invasion," said Goldsberry.

"So I dropped to the floor, told my boyfriend to get down-- there was somebody outside with a gun-- and I crawled to my handgun that was in the bedroom-- just because, as an OR nurse, I am trained, in emergencies, that, you know, you just do what you're supposed to do. [...] It's kind of like basic training-- so I thought 'someone's out there with a gun' I'm going to hide with mine in case he tries to come in.'"

Then the shouting began.

"We heard, 'open the door, it's the police'-- and I said to my boyfriend, 'that's not the police, the police don't point a gun at you from outside." And, as Goldsberry and her boyfriend noted, there was no indication that whoever was outside the door was law enforcement; no insignia was visible and no identification was displayed. "They looked like home invaders to us," said Goldsberry.

"They kept yelling, 'open the door,' then they said 'open the *fucking* door, this is the *fucking* police!' And, I yelled back, *'policemen don't say 'fuck!'*, or something like that-- because I was terrified."

According to Goldsberry, Dorris, who had remained standing by the front door, went to the window and stated that he wanted to see some identification. In response, rather than producing identification, or identifying himself in any way, the man at the door with the assault rifle opened the unlocked front door, stepped into the condo and pointed both a very bright light and the rifle into Goldsberry's face.

Seated on the floor, partially concealed behind a hallway wall, less than 15 feet from the intruder, Goldsberry raised her five-shot .38 caliber revolver and pointed it into the light. The two were "gun barrel to gun barrel," Goldsberry recalled.

"He was yelling at me, telling me to put down the f-ing gun, or he was going to f-ing shoot me [...]. So I said, 'I am an American citizen, I am trying to defend my home and my life'-- I was trying to reason

with this person, I guess, on a certain level."

It was during this tense moment that Dorris, who was still standing only feet from the front door and window, realized that the gunman was not alone and that there were in fact many heavily armed individuals running around outside the condo. According to Goldsberry, Dorris then raised his hands and asked if he could go outside and speak with the men.

The man with the rifle, who was later identified as U.S. Marshal Matt Wiggins, consented to Dorris' request. Upon exiting the condo, Dorris was handcuffed and detained.

Goldsberry remained inside the residence, shaking, crying and clutching her gun-- her miniature maltipoo (maltese/poodle mix) on her lap, growling at the invader. She did not know at that time what had become of Dorris.

"I was sitting there crying, because I didn't know what was going to happen to me next. I thought I was going to die. He-- Wiggins-- stepped back, outside my doorway, and I heard him say, 'we'd better get her out of there before she offs herself. And then that made me really angry, so I said, 'you don't have that kind of power over me.' Trying to make me feel like I'm crazy or something-- he put a gun to my face outside my condo."

Eventually, Goldsberry heard Dorris say, "honey, it's the police, put down the gun."

Goldsberry then put the gun in her closet, stood and stepped outside. She was handcuffed and detained for half an hour while officers (a mixture of Sarasota Police Department officers and U.S. Marshals) searched her home (without a warrant), emptied her gun of its ammunition and patrolled the Hidden Lake Village condominium complex, peering into the windows of her neighbors' homes just as they had her own.

During this period of detention, a marshal showed Goldsberry a picture of a man she had never seen before and had no knowledge of. The man, explained the marshal, was the man they were in search of -- and whom was believed to be in Goldsberry's condo.

Goldsberry recalled that during this time Dorris was held and interviewed by another marshal, who explained that an "anonymous phone tip" had led the officers to Goldsberry's door.

"Craig was thinking-- and later, when we were talking about it-- we're like, 'why would they mobilize six U.S. marshals, the SWAT team and SPD [Sarasota Police Department] from an 'anonymous phone tip'? But now, when I think back about the Stingray and the cell phone thing, maybe that's what he was referring to in an offhand way so we wouldn't know what he was talking about-- I don't know," said Goldsberry. "But, the thing is... my cell phone... I've never committed any crime, why would my cell phone be bringing them to this area? We don't know why they came here.... still."

SPD reports pertaining to the incident-- which Goldsberry characterizes as being "nothing but omissions and lies"-- do little to shed light on the circumstances of the raid. Upon review of the SPD field report of the incident, Goldsberry was shocked to find that officers stated they raided her home because there had been a "woman screaming" in the home at the time of their arrival. According to Goldsberry this is untrue-- as she never 'screamed,' and as the only shouting prior to Wiggins' entry

were those of *"open the fucking door, this is the fucking police!"*

However, the SPD Goldsberry home invasion report does contain an interesting factual admission; the report's "description" field simply states that SPD officers had been dispatched to "assist other federal agency."

According to Goldsberry, following the incident, SPD Chief Bernadette DiPino called her in order to 'reach out' and see if Goldsberry would join her for a cup of coffee (Goldsberry declined this offer). While the DiPino call fell short of an apology, Goldsberry said that DiPino stated her men were "just following the U.S. Marshals."

The U.S. Marshals Service (USMS) is an agency of the U.S. Department of Justice, tasked with apprehending fugitives from the federal criminal justice system, transporting and detaining federal prisoners, executing arrest and property seizure warrants/orders issued by federal courts, and providing security for federal courthouses. The recurrent word here, of course, is "federal." However, according to USMS' 2012-2016 Strategic Plan, the agency does also aid in the apprehension of "approximately 85,000 state and local fugitives through its vast network of fugitive task forces."

Indeed, U.S. marshal Wiggins, the man at the fore of the July 17, 2013 Goldsberry home invasion, is the agent-in-charge of such a fugitive task force, composed of USMS, SPD and other local law enforcement personnel.

The Goldsberry raid wasn't the only USMS joint fugitive task force mishap to occur in Sarasota on July 17, 2013. Earlier that day, members of the same task force tackled and handcuffed Elliot Stiner, a man employed as a cookie decorator at Westfield Sarasota Square Mall, as he waited for the bus after work.

The man sought by this USMS/local law enforcement fugitive task force in both the Goldsberry home invasion and the Stiner tackling was a Sarasota man by the name of Kyle Riley. Riley, then 25, was the subject of an arrest warrant, issued on July 8, 2013 by a criminal court of Florida's Twelfth Judicial Circuit, on charges of incest, sexual assault on a minor, and sexual assault and battery on a minor under the age of twelve. This later offense is a capital offense under Florida law and may be punishable by death or life imprisonment.

Riley was arrested in the early morning hours of July 18, 2013 in a part of town far removed from either Goldsberry's home or the Westfield Sarasota Square Mall.

When 'omissions and lies' fail... seize all the evidence

Following the July 17, 2013 incident, Goldsberry approached Sarasota civil rights attorney Andrea Mogensen.

Mogensen is a board member of the ACLU of Florida. ACLU of Florida Vice President Michael Barfield works as a legal consultant with Mogensen through her law firm, the Law Office of Andrea Flynn Mogensen.

Upon hearing the circumstances of the home invasion, Mogensen and Barfield began the groundwork for a civil suit against SPD and USMS. According to Goldsberry this suit is forthcoming, pending the

completion of a DoJ inspector General investigation of the incident.

Barfield said he developed a “very strong suspicion” that the Goldsberry and Stiner incidents involving the USMS/SPD fugitive task force stemmed from some form of cell site simulator error. As such, Barfield began making inquiries into the use of Stingray by SPD and USMS.

According to Barfield, he gained a confidential source during the course of these inquiries who was able to shed light on a “quid pro quo” arrangement between SPD and USMS involving the use of USMS' Stingray system.

As recounted by Barfield, his source stated that USMS had a longstanding cell site simulator technology sharing arrangement with SPD and other local law enforcement agencies. However, until recent years, USMS would only assist local law enforcement through the use of Stingray in urgent, truly exigent cases involving violent fugitives or suspects. According to Barfield's source, that all changed as USMS began to chafe under increasing evidentiary demands and scrutiny regarding cell site simulator use posed by judges in the federal court system.

So, USMS and local law enforcement struck a deal.

In exchange for more liberal use of the USMS Stingray system (no longer restricted to the most dire, or high profile cases), local law enforcement officers deputized as “Special Deputy U.S. Marshals,” would approach state courts in Florida's Twelfth Judicial Circuit and obtain trap and trace orders for the use of the USMS Stingray system-- thus avoiding the scrutiny of federal courts.

According to Barfield, his source laid it out like this:

“[The pursuit of Riley that resulted in the Goldsberry home invasion and the Stiner tackling] was a local case only-- no relationship to federal law at all [...] It used to be that [use of the USMS Stingray device] was reserved for, you know, very, very high profile wanted individuals-- murders, terrorists, et cetera. And, over the years, that standard-- that criteria, if you will-- has been watered down. We even have evidence of a situation where it was used in a minor felony and a misdemeanor [...] like a third degree felony-- it was a theft case-- it wasn't even a violent felony, it was a theft case, with a misdemeanor charge.”

“From what I'm told, the quid pro quo is 'we'll help you out in your local state investigations whenever you need it, as long as you help us out when we need it in our federal cases by going the state court judge route,' rather than the federal court-- because federal magistrate judges are apparently on to the agents about the use of the Stingray device and require a warrant. So, they are deliberately avoiding federal court because federal judges have caught on to what they are doing, and have said in many cases, 'you need a warrant for this kind of stuff'-- whereas, in state courts, the judges have not caught on yet,” added Barfield.

Through his inquiries, Barfield learned that SPD Detective Michael Jackson-- a detective who was part of the USMS fugitive task force (according to Barfield, Jackson was present at the Goldsberry home invasion), and who had been deputized by USMS-- was the point man at SPD for the acquisition of such orders.

On May 19, Barfield filed a public records request under Florida public records law (Florida Statues, Chapter 119) with SPD seeking records pertaining to Stingray, Stingray II and any agreements/leases with Harris Corporation.

Barfield then began approaching courts of Florida's Twelfth Judicial Circuit, seeking out records pertaining to trap and trace orders sought or obtained by Jackson. Through the course of these inquiries, Barfield learned that the courts retained no record of such orders sought or obtained by the detective. In short, Barfield found that Jackson somehow had managed-- for years-- to enter the court, obtain trap and trace orders, then leave the court with all evidence of his actions in his exclusive possession.

According to Barfield, this extraordinary control over any paper trail pertaining to Stingray use may be part of a larger effort to conceal the use of the technology.

“The problem with figuring out how many times this has occurred, and under what circumstances, is that the courts aren't retaining copies of these documents-- and they [USMS] know that. [Local law enforcement] are specifically told-- this is very important-- 'do not let any copies of those application or orders out of your custody'-- and, number two, 'if you're ever asked how information was discovered, that came from Stingray technology, you are to say 'confidential informant." The box-- Stingray-- is a 'confidential informant.' [...] It's a perfectly designed mouse trap,” said Barfield.

It is important to note here that both the federal Freedom of Information Act (FOIA) and most state public records laws contain broad exemptions allowing for the withholding of records pertaining to 'confidential informants.'

On May 22, Barfield approached Jackson and filed a second request (under Florida public records law), specifically seeking records pertaining to the acquisition of these trap and trace orders. Jackson confirmed that he was in possession of the records and an appointment was made for Barfield to inspect the records at Jackson's office at 2:30 on the afternoon of May 27.

That meeting, however, was not to occur.

At 12:20 p.m. on May 27, Barfield received an email from Assistant Sarasota City Attorney Eric Werbeck. In the email, Werbeck stated that Barfield's appointment with Det. Jackson had been cancelled. Werbeck provided a forwarded email, also dated May 27, between Werbeck and SPD Criminal Investigations Division Lieutenant Pat Ledwith, as rationale.

The forwarded email, written by Werbeck, read:

“I have discussed Mr. Barfield's request with the US Marshal's Service Office of General Counsel and the US Attorney's Office. We have been instructed not to release the documents requested, as any 'tap and trace' orders kept by Special Deputy US Marshal Jackson pursuant to his duties with the Marshal's Service belong to the Marshal's Service. The request should be made of the federal government through the Freedom of Information/Privacy Act.”

In response to Werbeck's May 27 email, Barfield asked Werbeck (both by email on May 28, and in a phone conversation on the evening of May 29) to affirm that a provision of Florida public records law (Florida Statutes, 119.07 (1) (h)), pertaining to the retention of responsive records, was being observed.

Florida Statutes, Chapter 119.0, Section 1, Paragraph (h) states:

“Even if an assertion is made by the custodian of public records that a requested record is not a public record subject to public inspection or copying under this subsection, the requested record shall, nevertheless, not be disposed of for a period of 30 days after the date on which a written request to inspect or copy the record was served on or otherwise made to the custodian of public records by the person seeking access to the record. If a civil action is instituted within the 30-day period to enforce the provisions of this section with respect to the requested record, the custodian of public records may not dispose of the record except by order of a court of competent jurisdiction after notice to all affected parties.”

On May 30, Barfield received the following email from Werbeck:

“The City's position is as discussed last night; the City never had custody of any orders, the US Marshal's Service maintained custody of them. After our phone call last night, I learned that the Marshal's Service had physically moved the subject record(s) from Sarasota to Tampa--though I am unaware of the location of any record(s) at this point.”

ACLU of Florida had been preparing a lawsuit, under Florida public records law, seeking to compel SPD's release of records responsive to the May 19 and 22 requests, when USMS seized records in SPD Det. Jackson's possession.

“They learned that we were getting ready to go to court, and they came and swooped in and picked the records up,” said Barfield-- who went on to state that in his 30 years of work concerning Florida public records law, he had never seen such a drastic action.

On June 3, the ACLU of Florida filed an emergency motion in Florida's Twelfth Judicial Circuit. This emergency motion served as a civil complaint against SPD and Det. Jackson. The complaint asserted that the City of Sarasota and SPD are agencies of the state of Florida, and, accordingly, are subject to Florida public records law. Among other things, the motion sought injunctive relief against the transfer of further documentation pertaining to Barfield's public records requests to USMS.

On June 17 Florida Twelfth Judicial Circuit Judge Charles Williams dismissed the suit.

Williams stated that neither Florida courts, nor Florida public records law, have any jurisdiction over the federal government, their agents, or records pertaining to their investigations (it should be noted, however, that no evidentiary hearing had been held in this matter prior to Williams' dismissal. As such, the plaintiffs had not been granted the opportunity to demonstrate that the Stingray and related trap and trace orders had been used by state/local agencies in state/local jurisdiction cases).

Williams opined that, due to the fact that SPD Det. Jackson had been deputized as “Special Deputy U.S. Marshal Jackson,” the records in his possession were property of USMS, and therefore subject to the federal Freedom of Information Act (FOIA)-- not Florida public records law. As such, said Williams, the issue of USMS' seizure of the Stingray records was “moot.”

Likely anticipating an appeal of Williams' dismissal on the part of the ACLU of Florida, the United

States Government (specifically the DoJ United States Attorneys Office), utilizing a rule of federal civil procedure, removed the case to federal district court. Under federal civil procedure the government has thirty days from the filing of the complaint in which to remove a case to federal court. Williams' dismissal of the case had occurred within that thirty-day window-- with time still left on the clock, so to speak.

Even though Williams had already dismissed the case, and even though the U.S. Government was not a party to the litigation (the sole parties in the case were the ACLU of Florida, SPD and Det. Jackson), the case was removed to United States District Court for the Middle District of Florida.

Currently, the ACLU of Florida is attempting to have the case remanded-- as it is a suit based in Florida law, concerning Florida agencies-- to the state court system for appeal.

Part 4: An End to the Rule of Law-- Harris Corporation/FBI/Tucson Police Department disregard for public and judicial oversight-- warrantless Stingray use-- the consequences of police militarization

In late April of 2013, I (Beau Hodai, publisher of *DBA Press*) learned, through a records request with the Arizona Department of Homeland Security (AZDOHS, a state entity that essentially acts as a bursar for U.S. Department of Homeland Security [DHS] grant funds paid out to state and local agencies) that, on June 30, 2010, the Tucson Police Department (TPD) had been reimbursed $396,500 through the DHS Operation Stonegarden grant program for their purchase of a Stingray II cellular tracking system from Harris Corporation.

Operation Stonegarden initiatives include narcotics, weapons, immigration and terrorism enforcement/interdiction.

On October 11, I filed a public records request, under Arizona public records law (Arizona Revised Statutes [ARS] 39-121.01 through 39-121.03), with TPD seeking, essentially, any and all records (including emails) pertaining to the department's use of the Stingray system; any and all records (including emails) pertaining to the Stingray system in any way; and any/all records (including emails) pertaining in any way to Harris Corporation.

On, or about, November 8, 2013, I received 20 pages of records from TPD in response to this request. TPD represented that these 20 pages were the complete fulfillment of the October 11 request.

However scant, the records disclosed a number of key facts:

The records disclosed that, in May of 2010, TPD purchased a Stingray II system, a Kingfish system, related software for both systems, as well as the Amberjack direction finding antenna and Harpoon power amplifiers. Records indicated that these pieces of equipment had been delivered to an entity referred to as the “Police Counter Narcotics Alliance.” These items totaled $408,500 in cost.

The “Police Counter Narcotics Alliance” appears to be the Counter Narcotics Alliance (CNA), a multi-jurisdictional entity in which TPD is active through a division of the TPD Investigative Services Bureau (TPD ISB).

According to a June, 2013 TPD organizational chart (the most current available), CNA consists of personnel from TPD, the Pima County Sheriff's Office, the Arizona Department of Public Safety (AZ DPS), Immigration and Customs Enforcement (an agency of U.S. Customs and Border Patrol, a DHS-component agency) and DoJ agencies DEA and FBI (the latter charged with investigative tasks within CNA related to "narco-terrorism" and-- ironically-- "public corruption"), and a number of other local law enforcement agencies.

According to the Arizona Criminal Justice Commission, CNA is a collaborative effort with a total of 18 participating agencies-- including agencies operating out of Davis Monthan Air Force Base.

The CNA mission statement describes CNA as "an interrelated drug and antiterrorism enforcement effort that shares resources and intelligence in the successful interdiction of illegal narcotics."

[It should be noted here, per jurisdictional claims/assertions arising out of the procurement and use of this Stingray system, that-- despite the involvement of so many federal "counter terrorism"/"homeland security" agencies in CNA, and DHS reimbursement for TPD's purchase of the technologies-- procurement records show that the Harris WPG technologies in the possession of TPD were procured by TPD/City of Tucson-- and TPD/City of Tucson alone-- and that they were delivered to a building owned by the City of Tucson.]

Most, if not all, of these CNA agencies are also active in the Arizona Counter Terrorism Information Center (ACTIC, commonly known as the "Arizona fusion center" *[for more on ACTIC and other "fusion centers," see "Dissent or Terror:" http://dbapress.com/archives/3121]*). ACTIC's primary coordinating state agency is AZ DPS, and the fusion center's chief coordinating federal agency is the FBI. According to ACTIC records obtained by *DBA Press*, there is a military intelligence component (largely Air Force Intelligence) of ACTIC operations as well. The stated focus of this military intelligence component is that of "narco-terrorism."

As such, the operations of these agencies through both CNA and ACTIC represent not only a broad multi-jurisdictional approach to "narco-terrorism" (appropriate to DHS Operation Stonegarden grant funding), but also as an excellent example of the erosion of jurisdictional boundaries between local/domestic law enforcement and military intelligence operations.

However, as TPD would later disclose, the Stingray II, Kingfish and other Harris WPG products were transferred out of CNA shortly following their purchase (if not immediately, upon purchase) and installed in the TPD Special Investigations Division (TPD SID, a division under TPD ISB) Home Invasion Unit (TPD HIU).

TPD Operations South Patrol Commander Lt. Kevin Hall was promoted from his position as the TPD sergeant in command of TPD HIU in February of this year. Prior to that point, Hall had served as the sergeant in command of TPD HIU from October of 2010 to February of 2014.

According to an affidavit submitted by Hall in defense of litigation stemming from TPD's failure to comply with the October 11, 2013 (and subsequent) public records requests, TPD HIU "has primary responsibility for investigation of all adult and suspected narcotics-related abductions of persons."

"As the supervisor of [HIU], I was primarily responsible for the use and maintenance of the Harris

equipment [...]. The purpose of acquiring this equipment was to assist in on-going abduction/kidnapping investigations."

Non-disclosure: corporate "competitive position" and litigious wrath, versus public interest

The most interesting pieces of information contained in the twenty pages of records delivered per the October 11 public records request, however, pertained to the redaction and withholding of records.

An email string, dated October 24, 2013, between then-TPD HIU Sgt. Hall and Principal Assistant Tucson City Attorney Lisa Judge indicated that, on October 22, upon compiling Harris WPG price lists, quotations of costs, purchase order and shipping invoices pertaining to the May, 2010 TPD purchases, Hall contacted Harris Corporation Contracts Manager Dawn Wheeler and provided Wheeler with these materials (presumably deemed to be the sole materials to be released pursuant to the October 11, 2013 request) for redaction.

In response, Wheeler provided Hall with a lengthy list of redactions to be applied to the materials. Causes given for these redactions were, variously:

FOIA exemptions pertaining to federal records describing law enforcement techniques (specifically under USC 552 (b) (7) et seq.); USC Title 18-- though no specific section was cited under USC 18, Harris had commonly claimed USC 18 2512 as grounds for non-dissemination of their "confidential" product brochures. This section of Title 18 pertains to restrictions on the publication of commercial advertisements for communications intercept devices; FOIA exemptions pertaining to federal records that may contain contractor "trade secrets" (USC 552 (b) (4)-- as described by Wheeler, disclosure of such records would "harm [Harris'] competitive position"); any extant FBI/TPD non-disclosure agreements (NDA); and a Harris WPG/TPD NDA.

A review of records delivered shows that the records were redacted as Wheeler requested.

The Wheeler/Hall/Judge emails concluded with an interesting final statement from Wheeler:

"As we discussed, you are currently in the process of having a new NDA signed with the FBI for your next purchase."

No further information pertaining to this "next purchase" or "new [FBI] NDA" was provided through materials delivered pursuant to the October 11 request-- though, clearly, any records pertaining to a Harris purchase, or FBI involvement in such a procurement, would have fallen under the scope of the October 11, 2013 public records request.

A copy of the Harris WPG/TPD NDA was attached to the email string and provided as part of the records set delivered per the October 11 request.

Before moving on to the provisions and implications of the Harris WPG/TPD NDA, it is important to note that-- as affirmed by TPD attorney Judge (in a recorded November 15, 2013 interview with myself)-- FOIA is not applicable to records in the possession of the Tucson Police Department; state agencies and the agencies of state political subdivisions-- such as the City of Tucson and its police department-- are subject to the public records laws of their respective states. FOIA applies only to

executive agencies of the Federal Government.

However, as asserted by Judge on November 15, the records delivered pursuant to the October 11, 2013 request were not redacted using FOIA-- they were redacted in accordance with the Wheeler requests for redaction (which, of course, were based on two rubrics: FOIA exemptions and the Harris NDA).

Illustrative of the deference shown to the wishes of Harris Corporation, during the November 15 interview Judge admitted that she, as the TPD attorney who oversaw and signed off on the processing of the October 11 records request, did not even know what material had been redacted:

"[...] We've signed a contract saying that we're going to keep certain information confidential, in exchange for them [Harris WPG] allowing us to purchase their product and use it [...] I don't even know what it [the information withheld] is because, frankly, they redacted it, so... I don't know what it is."

This admission casts a dubious light on subsequent TPD/City of Tucson assertions that they withheld records in the "best interest of the state"-- as opposed to the best interests of Harris Corporation's "competitive position."

The Harris WPG/TPD NDA, dated June 7, 2010 (and signed by City of Tucson and Harris on June 9 and 10, respectively, of 2010), states:

"Missions utilizing in whole or in part the Harris Products [including Stingray II, Kingfish and other Harris WPG products purchased by TPD] are covered in their entirety by this NDA.

"The City of Tucson is subject to this NDA and except for Court ordered or other judicially mandated disclosures, will not disseminate, publish or release any information about the operations, missions, equipment, CONOPS ["concept of operations"], mission or investigation results, methods or any other information related to or arising out of the use, deployment or application of the Products that would be deemed a release of technical data as it is described and agreed to under this NDA. In the event of a court ordered or judicially mandated disclosure, the City of Tucson shall use its best efforts to make such disclosure in a manner that provides maximum protection of the information to be exposed. [...]

"The City of Tucson shall not discuss, publish, release or disclose any information pertaining to the Products covered under this NDA to any third party individual, corporation, or other entity, including any affiliated or unaffiliated State, County, City, Town or Village, or other government agency or entity without the prior written consent of Harris [...]

"The City of Tucson is subject to the Arizona Public Records Law. A.R.S. 39-121, et seq. While the City will not voluntarily disclose any Protected Product, in the event that the City receives a Public Records request from a third party relating to any Protected Product, or other information Harris deems confidential, the City will notify Harris of such a request and allow Harris to challenge any such request in court. The City will not take a position with respect to the release of such material, beyond its contractual duties, but will assist Harris in any such challenge."

So, in a nutshell, the City of Tucson had signed a contractually-binding agreement with Harris WPG stating that A.) records pertaining to any/all investigations that employ Harris products-- even in part--

are now exempt from public disclosure; B.) the City will not disclose any detail of any piece of information pertaining to Harris WPG products to any other government agency-- of any kind-- without the express prior written consent of Harris; and 3.) the interests of Harris Corporation, as promulgated through the NDA, supersede Arizona Public Records Law (and the guarantee of transparency in government codified therein)-- and, in the event that some citizen files a request under state law seeking out some of that transparency, the City of Tucson is to turn their back on public law and support Harris Corporation (through the use of the City of Tucson's publicly-funded offices) in opposition to-- and even litigation against-- such a public records request.

On March 4, 2014, I, with the ACLU of Arizona as counsel, filed suit against the the City of Tucson and TPD in Pima County Superior Court, challenging TPD's failure to comply with Arizona public records law in their response to the October 11, 2013-- as well as TPD's complete failure to respond to two subsequent requests (also filed under Arizona public records law).

The subsequent requests were filed on November 15 and December 9, and sought, among other things, records pertaining to any court orders sought or obtained by TPD's in their use of the Harris technologies; records of communications with the FBI, including any/all FBI NDAs; records pertaining to Hailstorm; and any other records pertaining to the ongoing TPD Harris purchase mentioned in the Wheeler email.

On April 14, 2014 City of Tucson/TPD filed their response to the civil complaint. The assertion that disclosure of relevant records would hamper both domestic law enforcement/intelligence missions, as well as military/intelligence missions in the global 'war on terror,' stood at the heart of the City's response.

As stated by Judge during the November 15 interview, a piece of Arizona case law (a precedent established through Cox Arizona Publications, Inc. v. Maricopa County Attorney Tom Collins [*Cox v. Collins*], Arizona Supreme Court, 1993-- this piece of case law established that records pertaining to active police investigations are not necessarily exempt from requests filed under Arizona public records law; rather a balance of interests should be considered when determining the releasability of such records. In the end, Collins, who was seeking to withhold public records from various newspapers, lost the case) established three criteria for exemption of public records from disclosure under Arizona public records law: privacy (such as medical or personal financial records), confidentiality (argued by Judge to apply to contracts ensuring confidentiality, such as the Harris NDA), and those records, the withholding of which constitutes “the best interest of the state.”

It was the latter “best interest of the state” exemption that the city most forcefully asserted in the April 14 response. As was repeatedly iterated in both the response and accompanying law enforcement affidavits, disclosure of records pertaining to these investigative techniques would undercut the efforts of TPD, the FBI and all other agencies in locating kidnap victims and combatting “terrorism.” As stated in an accompanying FBI affidavit, disclosure of any information pertaining to cell site simulators would even “endanger the lives and physical safety of law enforcement officers.” As such, to compromise the TPD Stingray system through any degree of public transparency would not be in the 'best interest of the state.'

This argument as formally presented to the court, however, was markedly different in tone from Judge's initial assertions, made during the November 15 interview.

In that interview, Judge stated that she felt the *Cox v. Collins* "best interest of the state" exemption was appropriate rationale for TPD's non-compliance with the October 11 public records request. However, the primary concern cited by Judge at that time was not one of kidnapping or "counterterrorism." Rather, Judge stated that in that would not be in the "best interest of the state" for the City of Tucson to be sued by Harris Corporation for breach of their contractually-bound confidentiality, or to have Harris Corporation take TPD's Stingray system away.

To wit, when asked on November 15, 2013 which of the three *Cox v. Collins* exemptions she felt justified TPD/City of Tucson's actions, Judge stated:

"Confidentiality. Confidentiality, specifically-- because we have a, you know, binding legal contract, that, if we violate, we can be sued, and the stuff that we've spent money on, it can be taken away from us-- so definitely confidentiality. And I think, along with that, probably 'the best interest of the state'-- in avoiding litigation for violating the confidentiality contract, and stuff."

Interestingly, this wording didn't make it into TPD/City of Tucson's formal response to the civil complaint.

The great warrant hunt and admissions of Stingray use absent judicial oversight

But what of these assertions that the Stingray/Kingfish systems are vital in the location of kidnap victims and interdiction of terrorist acts? In order to attempt to fact check these assertions (some of which had been iterated in conversations with then-TPD Public Information Officer Sgt. Maria Hawke throughout October, November and December of 2013), through the fourth quarter of 2013 I sought out court orders used in such cases-- the intent being to verify the nature of offenses in instances of known Stingray use by the Tucson Police Department.

As had been stated-- emphatically-- by Hawke on a number of occasions throughout the fourth quarter of 2013, TPD sought and obtained "search warrants" (not pen/trap orders, as Hawke made very clear), specifically from Pima County Superior Court (Hawke was also very adamant about this detail), for the use of the Stingray/Kingfish systems.

However, when asked to produce any concrete instance of search warrant acquisition in junction with Stingray, or any identifying information pertaining to any case in which the TPD Harris WPG cell site simulators had been used, Hawke stated, variously: TPD communications pertaining to Stingray use are not retained; that Sgt. Hall had advised her that there is no "written work product" associated with Stingray use; that warrants are often sought telephonically, so there is no extant paperwork; that it would be impossible to locate warrants or cases associated with Stingray use, as Stingray is not identified by name in either the warrants or in the case files; that it would be difficult to locate cases or warrants associated with Stingray use, therefore Hawke would not attempt to locate such records; and that, in some cases, officers did not seek warrants, due to 'exigent circumstances.'

Realizing that TPD was intent on obfuscating their use of cell site simulators, I approached the Pima County Superior Court (PCSC).

Acting on my behalf, PCSC Public Information Officer Anne-Marie Braswell approached several

judges made inquires relating to warrants requested for use of Stingray or cell phone tracking technologies. According to Braswell, her inquiries came up empty; not a single PCSC judge was aware of any such request, nor were they familiar with the Stingray system (or any technology matching its description).

At one point, PCSC Grand Jury Clerk Darla Wandell stated that she believed a set of unsealed "tracking/search warrants" possibly pertained to cell phone tracking. However, upon review, these documents turned out to be warrants for the installation and use of GPS tracking devices (per *United States v. Jones*), clearly identifying the devices used, the placement of the devices on subject vehicles, and evidentiary information obtained through the use of the devices.

Given the fact that the tracking/search warrants clearly did not pertain to cell phones, both Wandell and Braswell were at a loss and suggested that pen/trap orders (all of which, according to Wandell, are automatically sealed in PCSC) would likely be the last remaining option in trying to assess Hawke's claims (if such orders could be unsealed). However, when asked for clarification on this matter, Hawke again asserted-- adamantly-- that TPD seeks *search warrants* for the use of their Stingray system.

Nevertheless, for all the weeks and months spent trying to ascertain whether or not TPD actually sought any judicial approval for their Stingray system, and what the nature of the investigations in those instances were, in their April 14 response to the civil complaint, TPD and the City of Tucson stated:

"Defendant does not seek pen registers in utilizing this technology, so there are no such records. Defendant is not aware that a search warrant has been sought by TPD to utilize the listed Harris Corporation technology within the relevant time period." [Note: the time period covered by the records request in question covered January 1, 2010 to October 11, 2013-- the entire duration of TPD's possession of the Stingray II and Kingfish systems, up to the date of the request's submission.]

And, in his affidavit accompanying the response, Hall stated:

"I am not aware of a use of this equipment by the Tucson Police Department wherein a warrant was obtained by the Tucson Police Department."

What was lost now is found: making sense of TPD reversals and obfuscations

TPD and the City of Tucson, through the April 14 response and associated affidavits, made some other interesting statements.

TPD claimed that, after being served with their copy of the civil complaint, they located various items responsive to the public records requests (though, for some reason, TPD does not admit that these identified items are, in fact, responsive to any of the three public records requests pertaining to these subjects submitted through the fourth quarter of 2013).

The newly-discovered items were: 1.) a PowerPoint training presentation for use with the Harris technologies (which was apparently created by Hall), 2.) an operational manual created by Harris Corporation, 3.) three "quick reference guides to calibration of the technology," 3.) a "blank form for a request to use the technology," and 4.) five case files for "the only five cases within the relevant time

period where the underlying technology has been used by TPD." [The time period covered by the records request in question covered January 1, 2010 to October 11, 2013-- the entire duration of TPD's possession of the Stingray II and Kingfish systems, up to the date of the request's submission.]

Of these five cases, TPD/City of Tucson stated that all but one had been closed.

In reference to this open fifth case, TPD/City of Tucson stated in a disclosure statement filed with the court on May 30:

"In the course of investigation to defend this lawsuit, Lt. Hall recovered a batch of raw data from an open investigation wherein this technology was utilized."

As previously stated, Stingray and related cell site simulators (including Kingfish and Stingray II)-- by their very nature-- force *all* cellular devices within their area of operation to communicate with them through forced registration, and then commence interrogation of *all* of these phones in order to obtain their MINs and ESNs. This step-- the forced registration and interrogation of *all* cellular devices within the Stingray's area of operation-- must be completed before Stingray can even begin to track a target phone. And, as previously stated, critics of cell site simulators argue that this activity is the digital equivalent to the very same acts of general search and seizure that served as the impetus for the creation of the Fourth Amendment. As such, critics of cell site simulators hold that their use-- with a warrant or not-- is likely unconstitutional.

Per Harris' FCC Stingray request, requiring that all "state and local law enforcement agencies must advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization," and given the FBI's evident interest in the TPD/City of Tucson lawsuit (this will be discussed at greater length shortly), it is logical to conclude that TPD is likely expected to follow DoJ guidance in their use of cell site simulators.

DoJ and their Federal Bureau of Investigation have long attempted to downplay and/or conceal the facts of Stingray interception and storage of data from "innocent" non-target cellular devices from both the public and the judiciary. However, due to Rigmaiden's attempts to compel disclosure of Stingray information through discovery in his criminal case, an FBI agent, Supervisory Special Agent (SSA) Bradley Morrison, chief of the FBI's Tracking Technology Unit, filed an affidavit in the U.S. District Court of Arizona on October 27, 2011. That affidavit provided a rare glimpse of FBI policy regarding Stingray use, as well as a number of disclosures as pertains to the interception of "innocent" data:

"FBI policy requires that at the conclusion of a location operation, FBI technical personnel are to purge all data stored in the pen register/trap and trace equipment. During a location operation, the electronic serial numbers (ESNs) (or their equivalent) from all wireless devices in the immediate area of the FBI device that subscribe to a particular provider may be incidentally recorded, including those of innocent, non-target devices. Purging is done by the FBI as an additional, internal procedural safeguard to ensure (1) that the privacy rights of those innocent third parties are maintained, (2) that the FBI does not store or maintain pen register/trap and trace data beyond the scope of its legal authorization, or (3) that the FBI does not collect information about individuals who are not the subject of criminal or national security investigations."

Yet, here we have a "batch of raw data" collected during an investigation that, by TPD's own

admission, falls under the timeframe of the October 11 request-- and which, by TPD's own admission, was gathered without either a search warrant or a pen/trap order (which means that, even though TPD claims this case is ongoing, there is no *"scope of legal authorization"* at all for the collection of this data, per Morrison's assertion that *"the FBI does not store or maintain [pen/trap] data beyond the scope of its legal authorization"*).

From these facts we can extrapolate that this raw data-- which, by its very nature would likely include data searched and seized from "innocent" cellular devices belonging to "individuals who are not the subject of criminal or national security investigations"-- has been in the possession of TPD since any time from January 1, 2010 to October 11, 2013 (the scope of the relevant request), to present. At a bare minimum (October 11, 2013 to the date of this disclosure, May 30, 2014) we are looking at retention period of eight months for this warrantless mass surveillance data.

Per TPD's claim that the five located case files are the sole instances of the department's Stingray use, consider this:

In his affidavit, Hall states that the Stingray/Kingfish systems are "rarely used" and that these five cases comprise the entire body of this $408,500 set of surveillance equipment's work product over a four-year period. TPD/City of Tucson allege the same in their response of April 14.

In his affidavit, Hall states that there is no information in any case file that identifies the use of the Stingray/Kingfish systems (apparently in spite of the template "blank form for a request to use the technology" located following the filing of the civil complaint), yet-- without any ability to reference the use of this technology-- TPD were somehow able to locate these five cases.

And, finally, TPD/City of Tucson and Hall both claim that TPD has never sought warrants or pen/trap orders for the use of the system. As such, if these assertions are true, there is no way to independently verify whether these five cases are, in fact, the extent of TPD's use of this technology.

Despite all of these assertions-- in which TPD asks both the public and the court to take it on faith that their Stingray system is just sitting on a shelf in TPD HIU gathering dust-- the City of Tucson and TPD state that they are in the process of upgrading their cell site simulator technology through a new purchase with Harris ("an upgrade of [TPD's] existing technology," as stated in the response. This is the "next purchase" referenced in the Wheeler/Hall email of October 22, 2013).

Given the fact that the only listed upgrades for Kingfish and Stingray II in the Harris GSA pricing schedule are upgrades to Hailstorm (an upgrade starting out at roughly $65K per unit), why would TPD be spending so much taxpayer money in upgrading surveillance systems they "rarely use"?

The consequences of police militarization

Another affidavit accompanied the April 14 TPD/City of Tucson response, that of FBI Tracking Technology Unit Chief, SSA Morrison.

Morrison's affidavit spoke largely to legal rationale perceived by the FBI to limit the release of Stingray-related public records.

But, before we go into the details of these assertions, it is important to note here that the FBI's standing in this case has not been established-- nor have any grounds for such standing been offered. Simply put, it is not known *what the FBI is doing in the room*, so to speak.

While it is true that Harris requested that the FCC require all law enforcement agencies seeking to purchase or use Harris WPG cell site simulators coordinate with the FBI; and while the Wheeler/Hall/Judge email discussed an ongoing TPD Harris WPG purchase, to involve a "new [FBI] NDA;" and while the Morrison affidavit states that "the FBI has entered into a [NDA] with our state and local law enforcement partners [...] specific to cell site simulator technology;" the April 14 TPD/City of Tucson response clearly states:

"Defendant does not currently have any non-disclosure agreement with the F.B.I. Defendant acknowledges that it is in discussions with Harris Corporation and the F.B.I. regarding an upgrade of its existing technology, which would include consent to a non-disclosure agreement with the F.B.I."

Yet, no such agreement currently exists.

Regardless of the FBI's lack of standing, TPD/City of Tucson disclosed in the April 14 response that all of the "newly discovered" documents, as well as the initial set of documents delivered pursuant to the October 11 request, had been submitted to the FBI for review-- and, in the case of the materials delivered pursuant to the October 11 request, redaction (under FOIA-- which, on November 15, Judge acknowledged had no bearing on the request, made under Arizona public records law).

In an apparent effort to sidestep this question of standing, the Morrison affidavit states that Morrison is "responsible for establishing and advising on policy guidance for the FBI [...]. This includes the use and deployment of electronic surveillance devices such as the cell site simulator at issue in this case."

Furthermore, throughout the affidavit, Morrison refers to the Harris WPG technologies as "the FBI's cell site simulator equipment." However, TPD's Harris WPG cell site simulator equipment was purchased by TPD, from Harris WPG, using (in part) DHS grant funding (FBI is not a DHS agency). Neither documents obtained from TPD or from AZ DOHS indicate that the FBI, or DoJ, had any role in TPD's acquisition of this equipment.

Nevertheless, Morrison's arguments against the disclosure of any portion of TPD's Stingray records run the gamut-- from the "categorical protection" "enjoy[ed]" by law enforcement techniques under FOIA (5 USC 552 (b) (7), which we will not discuss, as even TPD/City of Tucson Attorney Judge admits that FOIA has no standing in this instance); to dire consequences for the War on Terrorism/Kidnapping:

[Note: the following text is quoted from the FBI NDA that Morrison claims is typically entered into between the FBI and local law enforcement agencies, as quoted in the Morrison affidavit. Again, by TPD/City of Tucson's own admission, this NDA does not exist between FBI and TPD.]

"[Disclosing] the existence of and the capabilities provided by [cell site simulator equipment] to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation... to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law enforcement officers and other individuals, but also adversely impact criminal and national security

investigations. That is, disclosure of this information could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations' [...]

"Adding to the sensitive nature of the FBI's cell site simulator equipment, the same technologies and tools used in criminal cases are often used in counterterrorism and counterintelligence investigation. Thus, the compromise of the law enforcement community's investigational tools and methods in a *criminal case* [emphasis added: note the implications here for either judicial disclosure or defendant due process] or public records disclosure could have a significant detrimental impact on the national security of the United States."

In his affidavit, Morrison also claimed that cell site simulator technology is "homeland security information," exempt from disclosure under the Homeland Security Act of 2002 (HSA, one of the sweeping intelligence restructuring bills that was enacted in the wake of the events of September 11, 2001. This bill created the U.S. Department of Homeland Security).

"Specifically, any information shared by the federal government with a state concerning cell site simulator technology is considered homeland security information under [HSA]," wrote Morrison. "The Act defines homeland security information as information that relates to the ability to prevent, interdict, or disrupt terrorist activity; information that would improve the identification or investigation of a suspected terrorist or terrorist organization; or information that would improve the response to a terrorist act."

While it may be true that TPD's Stingray II, Kingfish systems and related technologies were financed in most part by federal DHS grants, there is no indication that either DHS or the FBI had any role-- other than as financier, in DHS' case-- in initiating the department's purchase or use of this cell site simulator technology.

Furthermore, if this provision of HSA were to apply to grant streams and technologies purchased through such grants-- as opposed to actual items of intelligence shared between agencies-- disclosure of any records pertaining to any equipment (from helmets, trucks, two-way radios and night vision goggles, to open source intelligence data mining systems and public safety radio dispatch equipment-- all of which are purchased under the banner of "counterterrorism" using DHS grant funding) would be barred from public disclosure. This simply is not the case.

Indeed, this cell-site-simulator-as-protected-counterterrorism-intelligence argument was literally thrown out of court when, on June 2, a Leon County judge in Florida's Second Judicial Circuit, ruled in favor of the ACLU of Florida's motion to unseal the suppression hearing transcript discussing Stingray use by the Tallahassee Police Department in *Florida v. Thomas*. In that instance, the State of Florida (arguing on behalf of the Tallahassee Police Department, the Florida Department of Law Enforcement and the FBI) also attempted to play the "counterterrorism" card through this HSA argument. The judge rejected this argument and ordered the transcript unsealed.

And, according to ACLU Speech, Privacy and Technology Project Staff Attorney Nathan Wessler, ACLU of Florida is in the process of reviewing 277 Tallahassee Police Department cases in which Stingray systems were used. In the course of this review, said Wessler, not a single instance cell cite simulator use in an investigation of a "terrorism"-related crime has emerged.

And so now we find ourselves entering into some truly dark waters.

In his affidavit accompanying the April 14 TPD/City of Tucson response, Morrison posited a new defense from disclosure of Harris WPG cell site simulator technologies to the public-- and, in particular, the press. This theory laid bare the implications of militarized domestic law enforcement.

We will let Morrison's words speak for themselves (all author's notes in this section emphasized) :

"*[C]*ell site simulator technology is a regulated defense article on the on the United States Munitions List (USML) (*[see Code of Federal Regulations pertaining to]* electronic equipment specifically designed for intelligence, security or military use in surveillance, direction-finding of devices which operate on the electromagnetic spectrum). As such, technical details concerning this technology are subject to the non-disclosure provisions of the International Traffic in Arms Regulations ("ITAR") *[...]* The ITAR implements the Arms Export Act *[...]* and Executive Order 13637 *[this is an executive order issued by President Barack Obama in March of 2013, pertaining to the regulation of arms exports]*, which control the export and import of defense-related articles and services listed on the *[USML]*. Because this equipment is explicitly governed by the ITAR, *[Code of Federal Regulations]* requires anyone, prior to making an export, to obtain a license from the Department of State. Notably, technical information does not have to leave the borders of the United States to be deemed an export subject to the regulation. (see *[Code of Federal Regulations]*, which defines an export as the disclosure of technical data about a defense article to a foreign national, even while located in the United States).

"Accordingly, if a state disseminates any part of the technical information knowing that a media organization intends to release the information to the public through the media or via a website, due to the accessibility of the information to non-U.S. citizens, or the requesting media organization employs or has any non-US citizens present at its offices, this may constitute a violation of the Arms Control Export Act. Any Unauthorized disclosure of ITAR-controlled information is a felony punishable by up to 20 years imprisonment and up to $1 million per occurrence."

This litigation is ongoing.

For their willingness to share information and insights, DBA Press thanks the following: Michael Barfield, Louise Goldsberry, Linda Lye, Chris Soghoian, Nate Wessler.