IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	**)**	
	)	
	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	**)**	
Defendant	**)**	

DEFENDANT'S REPLY TO GOVERNMENT'S RESPONSE MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A "GEOFENCE" GENERAL WARRANT

Okello Chatrie, through counsel, replies as follows to the government's response to his motion to suppress evidence obtained from a "geofence" general warrant. *See* ECF No. 29.

I. Obtaining Mr. Chatrie's Google location information was a search.

Mr. Chatrie presents two arguments as to why the government's acquisition of his Google location data was a search. The government responds to only one of them on the merits. First, Mr. Chatrie argues that the government's conduct was a search under the *Katz* reasonable expectation of privacy test. The government contends that he had no privacy interest in two hours of his location information, failing to appreciate the significance of the Supreme Court's landmark decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and seeking to create a *de minimis* exception to the Fourth Amendment. Second, Mr. Chatrie argues that it was a search under a property rights theory of the Fourth Amendment. This understanding of the Fourth Amendment predates *United States v. Katz*, 389 U.S. 347 (1967), and has been repeatedly identified by the Supreme Court as an equally valid and independent test. *See, e.g.*, *United States v. Jones*, 565 U.S. 400, 409 (2012); *Kyllo v. United States*, 533 U.S. 27, 37 (2001); *Soldal v. Cook County*, 506 U.S. 56, 62 (1992). The government, however, brushes it aside as if it were a recent invention of Justice

Gorsuch, offering no response on the merits. ECF No. 41 at 12. Under both theories, however, the acquisition of Mr. Chatrie's Google location data was a search.

A. Obtaining Mr. Chatrie's Google location information infringed on his reasonable expectation of privacy.

The government contends that Mr. Chatrie had "no reasonable expectation of privacy in any of the information disclosed by Google" because the location data covered two hours instead of seven days. ECF No. 41 at 6. But *Carpenter* did not gift the government a free pass from the Fourth Amendment for any such "limited period." 138 S. Ct. at 2220. On the contrary, the Court made it clear that it would not "grant the state unrestricted access to a wireless carrier's database of physical location information," describing such information as "deeply revealing," "comprehensive," and "inescapable" *Id.* at 2223. Mr. Chatrie had a reasonable expectation of privacy in his Google location information, which was at least as private as the records in *Carpenter*.

Carpenter involved two orders for historical cell site location information ("CSLI"): one seeking 152 days, and a second for seven days. 138 S. Ct. at 2212. In holding that a warrant is required for seven days or more of CSLI, the Court merely decided *Carpenter* on the facts before it. There is no higher constitutional significance to seven days, and *Carpenter* does not suggest that the Fourth Amendment would condone warrantless searches for a shorter period of time. In fact, the second CSLI order only produced only two days of records, not seven. *Id.* at 2212. Likewise, the Court did not express a view on real-time CSLI or "tower dumps" because those facts were not present in the record. *Id.* at 2220. But it would require misreading the rest of the Court's opinion to view this judicial restraint as an invitation to engage in warrantless surveillance. It is not enough to suppose, as the government does, that it might be possible to replicate this

location information given enough time and resources.[1] ECF No. 41 at 8. While some physical searches may be permissible without a warrant, the Court has been clear that "any extension of that reasoning to digital data has to rest on its own bottom." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

Applying the *Carpenter* framework, it is clear that obtaining Google location data was a search that infringed on Mr. Chatrie's reasonable expectation of privacy. Like the CSLI in *Carpenter*, Google location information is deeply revealing, comprehensive, and inescapable. 138 S. Ct. at 2223. It its revealing because it can expose the location of devices inside constitutionally protected areas, including "private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.* at 2218. Indeed, Google uses it for that very purpose when serving advertisements. Google Policies, Location Data (Nov. 20, 2018), https://policies.google.com/technologies/location-data?hl=en. And in this case, it located 11 users inside the Journey Christian Church, a quintessentially protected space that raises additional First Amendment concerns. *See Stanford v. Texas*, 379 U.S. 476, 485 (1965) (requiring courts to apply Fourth Amendment requirements with "the most scrupulous exactitude" when searches implicate First Amendment concerns).[2] In sum, two hours of Google location information is capable of revealing the same type of sensitive, private information as CLSI.

[1] Mr. Chatrie maintains that the data obtained through this warrant could not have been obtained through visual surveillance alone. In addition to subscriber information and account details, which are not observable, it would have been impossible to reconstruct all of the location data obtained from Google. Even if the government had unlimited time and resources, they would not be free to enter constitutionally protected spaces to log the devices located inside. Mr. Chatrie does not concede his privacy interest in the non-location data obtained through the geofence warrant.

[2] The government fails to adequately address these First Amendment concerns, just as it failed to recognize or address them when seeking a geofence warrant that fully encompassed a large church. The affiant simply described the church as "an adjacent business" without telling the Court that the "business" was actually a church.

The fact that the government obtained a smaller quantity of this location data than in *Carpenter* does not diminish its potentially revealing nature. *Carpenter* emphasized the long-term privacy implications of cell phone location tracking only because those were the facts before the Court. Elsewhere, the Justices have expressed concern with even short-term monitoring. In *United States v. Karo*, for example, the use of a beeper to track a drum of ether inside a private residence was sufficient to trigger Fourth Amendment scrutiny. 468 U.S. 705, 716 (1984) ("We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device . . . whether a particular article—or a person, for that matter—is in an individual's home *at a particular time*.") (emphasis added). Just a small window of GPS monitoring still creates a "precise, comprehensive record of a person's movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). Indeed, it takes little imagination to conjure the privacy implications of even a single trip to "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Id.* (quoting *People v. Weaver*, 12 N.Y.3d 433, 441-442 (2009)).

Far more troubling is the breadth of the search in this case. Whereas *Carpenter* concerned the search of just one person's location data, the geofence warrant authorized the search of an unlimited number of people's location data. Neither the government nor the magistrate knew in advance how many devices would be swept up as a result of the search. Indeed, the fact that it would yield information about 19 different devices was unknowable at the time of the government's application. This was not a problem the *Carpenter* Court had occasion to consider,

but it is one that has repeatedly troubled the Court.[3] Indeed, "dragnet" searches are a perennial Fourth Amendment fear. That is why the Constitution prohibits general warrants and requires both probable cause and sufficient particularity. Even if obtaining two hours of location data for a single person would not trouble the Court, obtaining two hours of data for every person in an area is a very different story. In this sense, it arouses the same fears of "too permeating police surveillance" and exercise of "arbitrary power" that motivated the *Carpenter* Court. 138 S. Ct. at 2214. Although the concerns in *Carpenter* are not identical, the potentially unlimited breadth of a geofence search makes up for the comparatively shorter duration of a geofence search. Consequently, the data obtained are highly revealing and deserving of Fourth Amendment protection, as much if not more so than the CSLI in *Carpenter*.

Similarly, Google location data has a comprehensive reach that is comparable to CSLI. In fact, CSLI *is* one of the data sources that Google collects and uses to determine users' locations. But Google also includes GPS location data as well as "additional information from nearby Wi-Fi, mobile networks, and device sensors." Google Policies, *supra*. As a result, Google location information is significantly more precise than CSLI alone. The government puts no stock in this distinction because the *Carpenter* Court "t[ook] account of more sophisticated systems" and recognized that CSLI "is rapidly approaching GPS-level precision." [G. at 8-9 (quoting *Carpenter*, 138 S. C.t at 2218-19).] But because Google uses multiple sources of location data, it locates devices even in places where GPS is unavailable or unreliable, such as indoors. If GPS data is not

[3]*See, e.g.*, *United States v. Knotts*, 460 U.S. 276, 284 (1983) (reserving the question of whether "different constitutional principles may be applicable" to "dragnet-type law enforcement practices"); *see also Jones*, 565 U.S. at 408 n.6 (quoting *Knotts*); *Karo*, 468 U.S. at 716 ("Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."); *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 327 (1972) (Douglas, J., concurring) ("[T]he recurring desire of reigning officials to employ dragnet techniques … lies at the core of [the Fourth Amendment]."); *Davis v. Mississippi*, 394 U.S. 721, 726 (1969) ("Nothing is more clear than that the Fourth Amendment was meant to prevent wholesale intrusions upon the personal security of our citizenry").

available, Google will then approximate location information based on the signal strength of known nearby Wi-Fi networks, which have a short range. Google is capable of doing this by referencing the billions of data points it gathers each day from other Android phones that report on the availability of Wi-Fi networks in range. *See* Tr. at 29, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019) (Ex. D). Only when Wi-Fi and GPS are unavailable does Google fall back to using CSLI, the least precise method. Consequently, Google location data is likely to be *more* comprehensive than GPS, locating devices where GPS is unavailable.

And finally, Google location data is "automatic and inescapable." For Android users like Mr. Chatrie, there is no practical way to avoid transmitting location information to Google, even if "Location History" is turned off. Location History only controls whether location data gets added to a user's "Timeline" feature, not whether Google sees or stores the data. Likewise, disabling Google Location Services does not actually stop a device from determining its location and creating a record. As Google explains, "Your device's location will continue to work even if GLS [Google Location Services] is turned off, but the device will rely only on GPS to estimate device location for apps with the necessary permission." Google Policies, *supra*. Those apps include basic, built-in Google services like Search and Maps. Thus, because "Google Location Services is distinct from your device's location setting," some location information still flows to Google even when it is off. *See* Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb. And while Google notes that there are separate controls for "Web & App Activity," this setting is isolated and unaffected by the restriction of other location information. Furthermore, the government is incorrect that Mr. Chatrie "had to affirmatively opt in" to sharing his location information with Google. As the user of an Android phone, Google Location Services is enabled

by default. *See* Verizon, Samsung Galaxy S9 / S9+ - Activate / Set Up Device, https://www.verizonwireless.com/support/knowledge-base-216675/ (showing Google location services on by default at step eight). Location History, by contrast, is an opt-in feature, but one that has no effect on the GPS, Wi-Fi, and other location data transmitted to Google through Location Services or Web & App Activity.[4] While it is technically possible to disable the phone's location functions altogether by activating "airplane mode" or powering off the device completely, such drastic steps are not required by *Carpenter*. 138 S. Ct. at 2220 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."). Rather, collection of Google location data is "inescapable" because, as in *Carpenter*, it relates to services one needs to be a functioning member of today's society. *Id*. In addition the ubiquity of Google services such as Search, Maps, and Mail, all Android phones—such as the one Mr. Chatrie had—run on Google's operating system and regularly transmit location data back to Google without any affirmative user action at all. The collection is therefore just as automatic and inescapable as CSLI.

In sum, Google location data is at least as revealing, comprehensive, and inescapable as CSLI. Thus, as in *Carpenter*, the fact that "such records are generated for commercial purposes . . . does not negate [Mr. Chatrie's] anticipation of privacy in his physical location." 138 S. Ct. at 2217. Mr. Chatrie had a reasonable expectation of privacy in his Google location data and obtaining those records was therefore a Fourth Amendment search. This is especially true because

[4] The government also draws a confusing and unsupported distinction between "incidental" disclosure of location information and disclosure as a "central prerequisite" to obtaining services. CSLI, however, is in fact essential to the use of a cell phone – required to route information to the correct tower and device. It is both central to the way cell phones function and a prerequisite to using their features.

of the "dragnet-style" search used to get them, a longstanding fear of the Court even when long-term surveillance is not at issue.

B. Obtaining Mr. Chatrie's Google location information infringed on his property rights in that data.

The *Katz* reasonable-expectation-of-privacy test has been in place since 1967, but the Supreme Court's Fourth Amendment jurisprudence is not so young. Throughout the late-19th and early-20th centuries, the Court hued closely to a literal reading of the constitutional text, focusing on the property rights attached to "persons, houses, papers, and effects." U.S. Const. amnd. IV; *see, e.g., Agnello v. United States*, 269 U.S. 20, 32 (1925) ("The search of a private dwelling without a warrant is in itself unreasonable and abhorrent to our laws."); *Weeks v. United States*, 232 U.S. 383, 391 (1914) (recognizing that the essence of a Fourth Amendment violation is "the invasion of his indefeasible right of personal security, personal liberty, and private property."); *Ex parte Jackson*, 96 U.S. 727, 732-33 (1878) (holding that postal mail is just as protected under the Fourth Amendment as those papers and effects kept in the safety of one's home). Indeed, the invasion of property rights was at the heart of Lord Camden's judgment in *Entick v. Carrington*, one of the pillars of English liberty and a catalyst for the Fourth Amendment. 19 How. St. Tr. 1029 (K.B. 1765) ("Papers are the owner's goods and chattels. They are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection"); *see also Boyd v. United States*, 116 U.S. 616, 626 (1886) (describing *Entick* as a "monument of English freedom" and "the true and ultimate expression of constitutional law"). On this side of the Atlantic, the founding fathers specifically designed the Fourth Amendment to assure security "in person *and property*" against unlawful searches. *Adams v. New York*, 192 U.S. 585, 598 (1904) (emphasis added). In short, the "traditional," property-based theory of the Fourth Amendment has a pedigree that long predates *Katz* and, given the Court's recent jurisprudence, is as valid as ever.

When the Court decided *Katz*, there was a palpable worry that property rights alone would not be sufficient to implement the Fourth Amendment in an age when communications could occur without an in-person meeting, but through electronic whispers miles apart. Justice Harlan embodied this concern in his famous concurrence, declaring that the Fourth Amendment protects "people, not places." 389 U.S. at 351. This understanding of the Fourth Amendment has served the Court well for decades, but it "did not repudiate [the] understanding" held for "most of our history" that the Fourth Amendment embodies "a particular concern for government trespass" on one's "papers" and "effects." *Jones*, 565 U.S. at 406-07.

Thus, for example, the Court in *Soldal* unanimously held that removal of a tenant's mobile home was a Fourth Amendment seizure even though the owner's "privacy" was not invaded. 506 U.S. at 62 ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). Likewise, in *Kyllo*, Justice Scalia avoided the *Katz* doctrine in finding that the use of a thermal imager on a home was a search. 533 U.S. at 37 ("The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."). Indeed, the *Kyllo* Court noted that "well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass." *Id.* at 40. And finally, in *Jones*, the opinion of the Court rested on trespass grounds. 565 U.S. at 404-05. The *Jones* Court found that placement of a GPS tracker on a car was a "physical intrusion" that "would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id*. Reaffirming *Soldal*, the *Jones* Court unequivocally stated that "the *Katz* reasonable-expectation-of-privacy test had been *added to*, not *substituted for*, the common-law trespassory test." *Id.* at 409; *see also Jones*, 565 U.S. at 414 (Sotomayor, J., concurring) ("*Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.").

Justice Gorsuch's dissent in *Carpenter* was a clarion call for courts and counsel to reassert the central role that property rights have played in the history of Fourth Amendment jurisprudence. 138 S. Ct. at 2272 ("Carpenter pursued only a *Katz* 'reasonable expectations' argument. He did not invoke the law of property or any analogies to the common law, … [and therefore] forfeited perhaps his most promising line of argument."). Mr. Chatrie does not ask this Court to adopt a novel theory, but to apply a deep-rooted one. *See id.* at 406-07. Mr. Chatrie takes Justice Gorsuch's warning seriously and seeks to fully assert his Fourth Amendment rights. The government, however, simply does not engage with the merits of Mr. Chatrie's property-based argument. ECF No. 41 at 12-13. Instead, the government chooses to ignore over a century of Fourth Amendment jurisprudence and merely quip that "a solo dissent is not the law." *Id.* at 12.

II. The warrant lacked probable cause and was even more unparticularized than previously thought.

The government responds that the geofence warrant was supported by sufficient probable cause and particularity. *Id.* at 13-21. But their arguments are even less persuasive in light of additional discovery showing that they twice requested additional location data on all 19 devices initially identified by Google, in contravention of the warrant itself. *See* Ex. A (First Step 2 Request) at 1; Ex. B (Second Step 2 Request) at 1. Indeed, Google twice rebuffed this request, ultimately sending additional information on nine devices. This development underscores why such an ad hoc, back-and-forth negotiation with the recipient of a warrant is no substitute for judicial oversight and a particularized warrant supported by probable cause.

More fundamentally, the government's response appears to misunderstand the significance of the Fourth Amendment's particularity requirement. Particularity is not just about how clearly a warrant identifies the object of a search for which there is probable cause to seize, but whether it adequately constrains law enforcement's discretion in the execution of that search and seizure. Its

basic purpose is to prevent general warrants by ensuring that "nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927). The government contends that the information it sought was "constrained" based on location, date, and time to the robbery under investigation. ECF No. 41 at 18. But it is not enough to simply name the crime and identify the general area where it occurred. Rather, such a warrant is more akin to the general warrant in *Wilkes v. Wood* that identified the crime of seditious libel but did not specify the places to be searched, the papers to be seized, or the persons to arrest. 98 Eng. Rep. 489, 490 (1763). Drawing a circle around the neighborhood to be ransacked does not change the analysis.

The government contends that the initial search ("Step One") satisfied the particularity and probable cause requirements because it specified information "directly tied" to a particular robbery, which of course occurred "at a particular place and time." ECF No. 41 at 13. But it failed to individualize its suspicion and tie that robbery to a particular account or accounts to be searched. That is like permitting the police to search for stolen goods in any place near a theft, to pat down every person in a bar where a crime had been committed, or to search every person in an apartment where illegal drugs may be present--all of which courts have found to be unconstitutional. *See Grumon v. Raymond*, 1 Conn. 40, 43 (1814); *United States v. Glenn, 2009 WL 2390353*, at *5 (S.D. Ga. 2009); *Commonwealth v. Brown*, 68 Mass. App. Ct. 261, 262 (Mass. App. Ct. 2007). It is also strongly reminiscent of the facts in *United States v. Curry*, in which this Court held that police did not have reasonable suspicion to stop Mr. Curry or any of the other men in a group after shots were fired in the general vicinity of where he was walking. No. 3:17CR130, 2018 WL 1384298, at *11 (E.D. Va. Mar. 19, 2018), *rev'd and remanded*, 937 F.3d 363 (4th Cir. 2019), *reh'g en banc granted*, No. 18-4233, 2019 WL 6133704 (4th Cir. Nov. 18, 2019) ("[G]eneralized suspicion and fear cannot substitute for specific and articulable facts . . . that support a

particularized and objective basis for suspecting *the particular person stopped* of criminal activity.") (internal quotations omitted). The government scoffs at the fact that "19 individuals, rather than hundreds or thousands" were affected by Step One of the warrant, ECF No. 41 at 18, but it gives no indication of how many bystanders would have to be searched before the collateral damage becomes too much for the Fourth Amendment to bear. Indeed, the government did not and could not have known how many devices would be affected by such a high-tech fishing expedition. The only thing certain at Step One was that law enforcement intended to search the Google data of many people who were *not* involved in the robbery.

It is not sufficient to respond, as the government does, that the location records of admittedly innocent people are the proper target of a search warrant on the off-chance that they might be useful in reconstructing the scene, identifying potential witnesses, or rebutting potential defenses raised by the robber. ECF No. 41 at 16. This argument proves too much. The issue is not whether there is some evidence to be had, but where the line is between a general warrant and a particularized one. The boilerplate speculation offered by the government would seemingly justify a search of anyone near any crime.

Moreover, the underlying reason the warrant lacks particularity is because the government does not have probable cause to search an unlimited number of unknown people who were near a crime. Probable cause is what makes particularity possible. Without it, there should be no surprise when a warrant also lacks particularity. As the government notes, the "information specified by a warrant must be 'no broader than the probable cause on which it is based.'" ECF No. 41 at 19 (citing *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006)). But here, the distinguishing feature of the warrant application is the absence of any identifiable suspects. Without some

individualized suspicion, it is trying to imagine how the resulting warrant would be anything other than unparticularized.

Contrary to the government's assertion, the warrant application established no probable cause for any of the Google data it obtained. Mere proximity to crime is not probable cause of criminal activity. The government points to the so-called "Playpen warrant" as precedent for its actions here, *Id.* at 20, but unlike the Playpen cases, there was no honeypot in this case—only a dragnet. The Playpen warrant was "based on probable cause to search any computer logging into [a child pornography website]." *Id.* at 20 (quoting *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016)). The suspicion generated as a result of logging in to such a website has been a critical element in decisions upholding that warrant's constitutionality. See, e.g., *Matish*, 193 F. Supp. 3d at 603 (finding that the "chances of someone innocently discovering, registering for, and entering Playpen were slim" because of the "numerous affirmative steps that one must take to even find Playpen on the Tor network" that make it "extremely unlikely for someone to stumble innocently upon Playpen"); *see also United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018) (noting that to access Playpen, a user must download Tor and enter a 16-character URL consisting of random letters and numbers, as well as enter a username and password to proceed past a welcome page that "was suggestive enough that Playpen's content would be apparent" to any visitor). In this case, however, there is no argument that using Google services or being near the Call Federal Credit Union is somehow inherently suspicious. Instead, a crime was committed, law enforcement had no suspects, and the government simply cast a dragnet. The prevalence of Android phones is not probable cause to search any Google users that happen to be nearby. And

the absence of any individualized suspicion, let alone probable cause, at Step One renders the entire warrant unconstitutional.[5]

The second phase of the warrant ("Step Two") fares even worse. The government asserts that the warrant was "remarkably limited" because it obtained the location information for nine individuals over a two-hour interval, regardless of whether they were inside or outside the 150-meter radius. ECF No. 41 at 13. Indeed, the government commends itself for seizing "less than the maximum quantity of location and identity information that the warrant authorized." ECF No. 41 at 18. But this argument only gives lie to the entire three-step process. According to the government, the warrant authorized the government to seize "identity information and two hours of location data for *all individuals* present at the site of the robbery during the hour of the robbery." *Id.* at 19 (emphasis added). The warrant, however, is not so clear on this point.

The impression one gets from reading the warrant application is that the three-step process matters—that it is a means of protecting the privacy of bystanders by using "anonymized"[6] data to "narrow down the list" before obtaining additional records in Step Two, and then de-anonymized identity information in the third phase ("Step Three"). But the government, in its requests to Google and in a careful reading of Attachment II, said that they were actually entitled to Step 2 and Step 3 data on *everyone* snared in Step 1, no narrowing required. The warrant only says that law enforcement will "attempt" to narrow the list in Steps 2 and 3. *See* Warrant

[5] The government invites this Court to "sever the second step of the warrant and to suppress second-step information" only, ECF No. 41 at 20, but to do so would condone the digital equivalent of a general warrant that lacked particularity from the outset. *See, e.g., United States v. Sells*, 463 F.3d 1148, 1158 (10th Cir. 2006) (noting that "every court to adopt the severance doctrine has further limited its application to prohibit severance from saving a warrant that has been rendered a general warrant by nature of its invalid portions despite containing some valid portion").

[6] Mr. Chatrie does not concede that this data is not personally identifiable.

Attachment I at 1-2; Warrant Attachment II at 2-3. The verb "attempt" appears six times, doing quite a lot of work.

The government did in fact request the "maximum" amount of data—twice. In two emails to Google following the production of Stage One records, the government asked for "additional location data and subscriber info" for all 19 devices identified in step one. *See* Ex. A at 1; Ex. B at 1. Google did not respond to either of these requests. It was not until the government sent a third email requesting additional data on just nine devices that Google produced more records. *See* Ex. C (Third Step 2 Request) at 1. This is not to suggest that the government did not "attempt" to narrow down the list. Indeed, the government twice tells Google, "If this request seems unreasonable, please keep in mind that device numbers 1-9 may fit the more likely profile of parties involved," but then requested additional information on all 19 anyway. *See* Ex. A at 1; Ex. B at 1.

It is unclear whether the practical realties of the three-step process were apparent to the issuing magistrate. It was certainly not clear to Mr. Chatrie prior to reviewing the negotiations between Google and law enforcement over the data to be produced in Step Two. The critical point, however, is that it was up to Google to decide whether the additional search was "reasonable." *Id.* That is a question that the Constitution makes clear is for a neutral and detached magistrate, not Google. *See Groh v. Ramirez*, 540 U.S. 551, 561 (2004) ("Even though [law enforcement] acted with restraint in conducting the search, 'the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.'") (quoting *Katz*, 389 U.S. at 356). In reality, the government would have obtained the "maximum" amount of data authorized had Google not enforced the warrant's strong suggestion that law enforcement should be required to first "narrow down the list." *See* Ex. A at 1; Ex. B at 1. Google, not the government, deserves commendation

for somewhat limiting the scope of this dragnet search—but it is not and should not be their job to do so.

Put simply, the government lacked probable cause to search any individual's location data, so law enforcement sought to search a broad swath of everyone's data in the area of the robbery. Without sufficient probable cause, the warrant was doomed from the start, as further evinced by its equal lack of particularity. The government's "attempt" to "narrow down the list" was merely cosmetic, masking its multiple grabs for the "maximum" amount of data that it believed investigators was entitled to. Law enforcement's emails to Google clearly demonstrate how the government viewed the three-step process as no more than window dressing. Instead, the government put Google in the role of magistrate, deferring to Silicon Valley to determine what was "reasonable." *See* Ex. A at 1; Ex. B at 1. Such a delegation of constitutional authority is contrary to the Fourth Amendment, demonstrating the profound absence of probable cause or particularity in this case.

III. The warrant was *void ab initio*.

The government seeks to sidestep the unlimited breadth of the warrant by arguing that Mr. Chatrie "lacks standing to challenge the government's acquisition of others' location information." ECF No. 41 at 12. But Mr. Chatrie is not asserting the Fourth Amendment rights of others; he is asserting his own. The unlimited breadth of the warrant bears directly on its absence of particularity, rendering it an unconstitutional general warrant that was *void ab initio*—invalid from the beginning. *See Groh*, 540 U.S. at 558 (finding a warrant "so obviously deficient" in particularity that "we must regard the search as 'warrantless' within the meaning of our case law.").

The history of the Fourth Amendment and the framers of the Constitution make this very clear. For example, "[w]hen James Otis, Jr., delivered his courtroom oration against writs of

assistance in 1761," he argued that "the writs … were void as a form of general warrant." *Payton v. New York*, 445 U.S. 573, 608 (1980) (White, J., dissenting). Lord Camden's judgment in *Entick*, one of the pillars of English liberty and a catalyst for the Fourth Amendment, similarly held a general warrant to be "illegal and void." 19 How. St. Tr. 1029; *see Boyd*, 116 U.S. at 616 (citing this holding and noting that "the principles laid down in [*Entick*] affect the very essence of constitutional liberty and security."); *State Tax Comm'n v. Tenn. Coal, Iron & R. Co.*, 89 So. 179, 182 (Ala. 1921) (noting *Entick*'s holding that "the general warrants issued by the Secretary of State were, under such circumstances there outlined, declared illegal and void."). And when a warrant is void, "potential questions of 'harmlessness'" do not matter. *United States v. Krueger*, 809 F.3d 1109, 1123 (10th Cir. 2015) (Gorsuch, J., concurring). The geofence warrant violated Mr. Chatrie's Fourth Amendment rights, not just the rights of bystanders.

IV. The good faith doctrine does not apply.

The *Leon* good faith exception to the exclusionary rule does not apply to evidence discovered as a result of an arrest premised upon a warrant that was *void ab initio*. As the *Leon* Court explained, "in so limiting the suppression remedy, we leave untouched the probable-cause standard and the various requirements for a valid warrant." 468 U.S. 897, 923-24 (1984). Thus, the good-faith exception is inapplicable to warrants that do not meet the probable cause and particularity requirements. While the Fourth Circuit has applied the good faith exception to warrants authorized by magistrates lacking jurisdiction, *McLamb*, 880 F.3d at 691, the Circuit did so because suppression would not have appreciably deterred police misconduct. *See United States v. Seerden*, 916 F.3d 360, 367 (4th Cir. 2019). By contrast, the Fourth Circuit has never applied the good faith doctrine to a general warrant, as suppression serves the goal of deterring police from seeking such intentionally overbroad and unparticularized warrants in the future. *Leon* may excuse

a deficiency in the language of a warrant that is subsequently invalidated, but it cannot excuse a general warrant that is void at its inception. To hold otherwise would incentivize the kind of "systemic error" and "reckless disregard of constitutional requirements" that the Supreme Court has cautioned against. *Herring v. United States*, 555 U.S. 135, 144 (2009).

Even if *Leon* were to apply in this case, evidence from an unconstitutional search should still be suppressed in at least four circumstances, three of which are relevant here. *See United States v. Leon*, 468 U.S. 897, 923 (1984).

First, magistrate issuing the geofence warrant "abandoned his judicial role" by granting immense discretion to the executing officers to decide what Google data to search, and so "no reasonably well trained officer should [have] rel[ied] on the warrant." *See id.* (citing *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319 (1979)). *Lo-Ji Sales* determined that a "Town Justice" abandoned his judicial role when he accompanied the police to execute a warrant for obscene material at a store and granted the police immense discretion in seizing materials. 442 U.S. at 326-27. "When he ordered an item seized because he believed it was obscene, he instructed the police officers to seize all 'similar' items as well, leaving determination of what was 'similar' to the officer's [sic] discretion." *Id.* at 327. "The Fourth Amendment does not permit such action," nor such "open-ended warrants." *Id.* at 325. Among other problems, this grant of discretion prevents the magistrate from "verify[ing] that the inventory prepared by the police . . . accurately reflected what he had ordered seized." *Id.* at 327. Here, the warrant left it up to law enforcement and Google to decide which devices would be subject to further search in Steps 2 and 3. "The Fourth Amendment does not permit such action," reserving this function for the judiciary. *See id.* at 325. Here, the court would have no way of determining whether the data obtained in Steps 2 and 3 "accurately reflected" what the magistrate had ordered seized because there were no separate court orders

authorizing them. Instead, it was effectively an "open-ended warrant," *id.*, in which the magistrate abandoned his judicial role.

Second, the good faith exception should not apply because the government's generalized assumptions about cell phone use rendered the geofence warrant "so lacking in indicia of probable cause" to search Mr. Chatrie's data that "official belief in its existence [was] entirely unreasonable." *See Leon*, 468 U.S. at 923 (internal citations and quotations omitted). In *United States v. Doyle*, for example, the Fourth Circuit Court of Appeals held that good faith did not apply when the police searched a house for child pornography with a warrant that contained "remarkably scant evidence … to support a belief that [the defendant] *in fact* possessed child pornography." 650 F.3d 460, 472 (2011) (emphasis added). The district court incorrectly "opined that '[t]he magistrate could reasonably infer'" this possession from the affidavit's recitation of allegations of sexual assault by children and second-hand allegations of possession of child pornography. *Id*. at 471-72. In *Seerden*, by contrast, good faith did apply where the affidavit contained allegations and admissions of the actual crime for which evidence was sought (sexual assault). 916 F.3d 360, 367-68 (4th Cir. 2019). Here, the police presented no evidence that the robber "in fact" had a smartphone, used Android or Google services, and opted-in to location services, and thus that his data was "in fact" in Google's Sensorvault. *See Doyle*, 650 F.3d at 472; ECF No. 41 at 14. Per *Doyle*, this Court cannot "reasonably infer" this fact from the government's generalized assumptions about cell phone use and should instead hold that any "belief in [the] existence [of probable cause for the warrant was] entirely unreasonable." *See Doyle*, 650 F.3d at 471; *see Leon*, 468 U.S. at 923.

Third, good faith should not apply because the geofence warrant was "facially deficient." *See Leon*, 468 U.S. at 923. It sought unfettered discretion to search deeply private data of an

unlimited number of people, and was so lacking in probable cause and particularity that "the executing officers [could not have] reasonably presume[d] it to be valid." *See id*. The government's attempt to evade this problem with *McLamb* is unpersuasive. In *McLamb*, the court found that "the boundaries of a magistrate judge's jurisdiction in the context of remote access warrant" was not clear at the time the agent applied for the warrant. 880 F.3d at 691. In those very limited circumstances, the court looked to the agent's consultation with attorneys from a specialized section within DOJ as evidence of good faith. Here, the watershed decision in *Carpenter* provided significant guidance for officers in this case. This Court cannot allow a reference to consulting with a government attorney to subsume the Fourth Amendment's requirement that a neutral and detached magistrate decide whether to issue the warrant.

As the Supreme Court recognized many decades ago, the Fourth Amendment requires a "neutral and detached" judge to find probable cause because the investigating officers are engaged in "the often competitive enterprise of ferreting out crime." *Coolidge v. New Hampshire*, 403 U.S. 443, 449 (1971). "[T]he whole point of the basic rule . . . is that prosecutors and policemen simply cannot be asked to maintain the requisite neutrality with regard to their own investigations—the 'competitive enterprise' that must rightly engage their single-minded attention." *Id.* at 450. Thus, it is the role of only the courts to enforce the constitutional requirement of particularity. To adopt the government's position here that consulting with members of the prosecution team is sufficient to establish good faith would completely eviscerate a clear protection that the Fourth Amendment in its own words requires.

CONCLUSION

The geofence warrant in this case was a general warrant, devoid of the probable cause and particularity required by the Fourth Amendment, the unconstitutionality of which should have been

readily apparent. For the foregoing reasons, Mr. Chatrie requests that this Court find the warrant void and suppress all of the fruits thereof.

Respectfully submitted,

OKELLO T. CHATRIE

By: _____/s/_____

Michael W. Price
NY Bar No. 4771697 (pro hac vice)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

_____/s/_____

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on December 9, 2019, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

/s/

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472
Importance: High

Google Legal Team,

I'm writing to inquire about my correspondence with your office on 07/01 and 07/02. Please keep in mind that expedition is requested based on armed and dangerous subject(s) still being at large. Subject was on cell phone just prior to violent act; therefore, Google may have captured pertinent information to identify and arrest parties involved. See below:

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

As discussed yesterday over the phone, I appreciate your quick response and willingness to provide GPS data for the below device ID(s). Please expedite this request where possible due to this suspect's continued threat to our community. If it would speed up the process, please provide data as it becomes accessible/available, starting with device ID(s) 1 – 9. It was mentioned that the larger the request, the more time it will take to get data back. With this in mind, I will still have to rule out device ID(s) 1-9; however, I may be able to do so more quickly if I can begin reviewing data. The faster I can review the data, the faster I can get this guy/guys off the street.

Thanks again for your professionalism and understanding. I realize that I'm asking for a lot and you and your team are likely tasked-out already, but any and all assistance and expedited process is MUCH appreciated.

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

[redacted]

"If you only do what you can do, you will never be better than what you are now."

VIRGINIA:

IN THE CIRCUIT COURT FOR THE COUNTY OF HENRICO

- -:

COMMONWEALTH OF VIRGINIA,	:	Case Nos.:
Plaintiff,	:	CR17-4909-00F
vs.	:	CR17-4910-00F
	:	CR17-4911-00F
ROLAND E. ANDERSON,	:	CR17-4913-00F
Defendant.	:	

- -:

Transcript of the proceedings in the above-styled matter, when heard on January 4, 2019 before the Honorable Richard S. Wallerstein, Jr., Judge.

CRANE-SNEAD & ASSOCIATES, INC.
4914 Fitzhugh Avenue, Suite 203
Richmond, Virginia 23230
Tel. No. (804) 355-4335

APPEARANCES:

Matthew C. Ackley, Esquire
Deputy Commonwealth's Attorney
Sarah E. Ulmer, Esquire
Assistant Commonwealth's Attorney
County of Henrico, Virginia
4301 East Parham Road
Post Office Box 27032
Richmond, Virginia 23273
Counsel for the Commonwealth

Matthew T. Mikula, Esquire
GILLIAM & MIKULA PLLC
7821 Ironbridge Road
Chesterfield, Virginia 23832
Counsel for the Defendant

INDEX

E X H I B I T S

THE CLERK: Commonwealth of Virginia versus Roland Ellisworth Anderson, case numbers CR17-4909, 4910, 4911, and 4913-00F.

THE COURT: Good morning to you, sir. Are you Roland E. Anderson III?

DEFENDANT ANDERSON: Yes, sir.

THE COURT: The record will so reflect. You may have a seat, sir. Mr. Mikula, good morning.

MR. MIKULA: Good morning.

THE COURT: Mr. Ackley, good morning. Ms. Ulmer, good morning again.

MS. ULMER: Good morning.

THE COURT: The matter is set for eleven o'clock today January 4, 2019 by the clock it's 10:52, any objection to starting a few minutes early Mr. Mikula?

MR. MIKULA: No, sir.

THE COURT: And on behalf of the Commonwealth, Ms. Ulmer?

MS. ULMER: No, sir.

THE COURT: All right. This comes before the Court by way of Defendant's motion in limine. How would you folks like to handle that issue?

MS. ULMER: Your Honor, the Commonwealth agrees with the Defense that it is the Commonwealth's burden so we are happy to go with that.

THE COURT: Treat it much like a motion to suppress and the Commonwealth to go first?

MR. MIKULA: That's fine.

THE COURT: That works for you Mr. Mikula?

MR. MIKULA: Yes, sir.

THE COURT: All right. On behalf of the Commonwealth, Ms. Ulmer?

MS. ULMER: Yes, sir, your Honor. Your Honor, at first the Commonwealth would like to submit Commonwealth's Exhibit number one, the raw DVD video, which we will be using in our presentation. It has been provided to the Defense.

THE COURT: Any objection?

MR. MIKULA: No objection.

THE COURT: All right. That looks like it's a DVD or CD?

MS. ULMER: Yes, sir.

THE COURT: Okay and will it work if the Court places the exhibit sticker on the disk itself as opposed to on the sleeve?

MS. ULMER: Yes, sir.

MR. MIKULA: I've printed off hard copies as well that I can administer.

THE COURT: I would prefer to put it on the disk if it turns out that somehow or another it doesn't work, it doesn't allow it to be played on the disk, I'll remove the exhibit sticker

and put it on the envelope.

MR. MIKULA: Yes, sir.

THE COURT: Marked as Commonwealth's Exhibit number One and return it to the Commonwealth, Deputy.

NOTE: Commonwealth's Exhibit 1.

THE COURT: Thank you. Ms. Ulmer?

MR. ACKLEY: Actually, I don't think we need that exhibit. It can just be introduced into evidence.

THE COURT: All right, thank you. Commonwealth's One.

MS. ULMER: Your Honor, the first witness is Jeremy D'Errico.

THE COURT: I'm sorry Jeremy?

MS. ULMER: D'Errico.

THE COURT: Mr. D'Errico, please.

THE DEPUTY: Would you step up to the witness stand for us, please?

THE COURT: Watch your step as you step through the opening and when you have a moment, would you raise your right hand? Do you swear or affirm the testimony you're about to give is the truth, the whole truth and nothing but the truth?

WITNESS D'ERRICO: I do.

THE COURT: You can have a seat.

WITNESS D'ERRICO: Thank you.

MS. ULMER: Your Honor, Agent D'Errico has prepared a presentation today. I've given a hard copy to Mr. Mikula. It is going to be displayed on the television but I also have a hard copy for your Honor if you would like to look at that.

THE COURT: All right, any objection Mr. Mikula?

MR. MIKULA: No, sir.

THE COURT: All right, I'll be happy to review and receive the hard copy. That's not an exhibit, this is for simply demonstrative purposes, is that correct?

MS. ULMER: Yes, demonstrative or a visual aid.

THE COURT: Okay. The witness has been sworn.

MS. ULMER: Thank you.

SPECIAL AGENT JEREMY A. D'ERRICO, the witness, having previously been duly sworn, testified as follows:

DIRECT EXAMINATION

BY MS. ULMER:

Q Agent D'Errico, can you please state your name for the Court?

A Good morning. My name is Jeremy D'Errico. The

last name is D-apostrophe-capital E-R-R-I-C-O.

Q And I've already called you Agent but how are you employed?

A I'm a Special Agent with the Federal Bureau of Investigation.

Q How long have you been employed by the FBI?

A Approximately six years.

Q And how do you, before being in your current position, have you held any other positions with the FBI?

A Yes, so I'm currently a Special Agent. I've been a Special Agent for the past four years. Prior to being a Special Agent, I was a computer scientist for the FBI for two years.

Q And where did you receive your education?

A My undergrad is a Bachelor's of Science or a Bachelor's of Science in Computer Science from James Madison University. And I also have a Master's of Information Security from the Johns Hopkins University.

MR. MIKULA: For purposes of the record, we're willing to stipulate to his expertise as a digital forensics expert.

THE COURT: Is that acceptable with you?

MS. ULMER: Judge, just in the chance of appeal, your Honor, we'd like to go through a little more questions.

THE COURT: All right.

MS. ULMER: Just to qualify him but I appreciate

Mr. Mikula's motion.

THE COURT: Please proceed.

BY MS. ULMER:

Q What team are you currently a member of at the FBI?

A I'm assigned to the Richmond division and assigned to the violent crimes squad. This case in particular I investigate organized crime. But I also handle threats to life, bank robberies, other violent crime matters as well as an additional duty, the CAST team, which is the Cellular Analysis Survey Team.

Q And before you came to the FBI, did you work anywhere else?

A I did. I worked for about seven years for the Meyer Corporation. And as part of the Meyer Corporation I was an information systems engineer where I was detailed to the FBI to investigate some of the largest criminal cyber matters dealing with large quantities of data.

Q And you mentioned the CAST team that's what you currently are on, could you please explain to the Judge what CAST is?

A The CAST team, the Cellular Analysis Survey Team. We're a team of approximately 75 Special Agents or task force officers located throughout the world. And we are specially

trained in analyzing historical cell site records and providing analysis of tower locations and where telephone calls may or may not have been placed. The CAST team is specially trained. All of us have in excess of 300 hours of specific training, which may include radio frequency analysis, training from the major telecom providers, their network engineers and their custodians of records so that we understand how these records are collected and how their networks work. We also receive training from academic instructors both Bureau instructors and from the private sector.

Q And so you've already touched on this but do you receive training directly through cell phone providers as well?

A We do. We receive training from Verizon, Sprint, AT&T, US Cellular and T-Mobile.

Q And before you become a CAST member, do you have to pass a written test?

A I do. And we're evaluated throughout the course of our training. So our training starts off with a week of basic training, which is how to understand these records and how to plot them on maps. The top performers from that class move on to the advanced training class where we deal with more of the same. Top performers from that class move on to the field training exercise where we are doing multiple analyses a day and going out and working historical cases, where we know phones were found. And then we move on to the two-part

certification each two weeks where we meet and train with the different providers on their networks and the academic instructors.

Q Once you become a CAST member, do you have to recertify every year or do you maintain that status?

A We do. We recertify every year. We take approximately forty hours of training each year in order to refresh on new technologies and to make sure that we still have a good understanding of our trade craft.

Q Approximately how many cases of historical cell site requests does CAST receive every year?

A We received I believe it was about 1700 since the inception of CAST, which started in 2010. Last year alone, or FY17, I think we are up to 300 cases alone. We provided expert testimony on 300 occasions in 2017 in courts similar to this.

Q Is that courts in the entire country or?

A That's across the country, both federal, state and local courts.

Q And you, yourself, have you ever testified in an expert capacity in Virginia state courts?

A I have as to Google location records and that was in Henrico County on three occasions last year.

Q Can you briefly explain to us what exactly historical cell site analysis is?

A Yeah, historical cell site analysis is matching up the call detail records and the cell site information that's provided by the carriers to a tower list that's provided by the carriers. So the carriers document where all their towers are and the directions of their antennas so that we can take that information and marry it up with the call detail records. That tells us the starting tower of that phone call and the ending tower of that phone call and we can place that, an indication on the map of the approximate location of the mobile device, the phone when it was making that call.

Q So when you get historical cell site analysis, how do you use that analysis, what do you use that to determine?

A We determine the approximate location of the phone at that time. And we cannot get it down to a room in a house. But we can tell an approximation of where that phone may have been during that transaction. And that can be a call or a text message or a data transaction.

Q As a CAST member, how do you apply your knowledge of historical cell site data to what you are asked to do for the FBI?

A They are very similar. So both the cell sites and the collection of GPS and Wi-Fi data, they both depend on radio frequency analysis. We were provided records by Google to review and analyze and Google has provided certain information for us to be able to plot those records on a map,

along with what they call an accuracy radius of the approximation of where they believe that phone was.

Q And can you use that information in order to locate fugitives?

A Yes, we can and we have in the past.

Q How else have you used that information?

A We've used that information to help find missing children, used that to help find fugitives that are fleeing from the law. We have used that information in numerous ways and corroborate that information as much as possible, whether that be witness statements or other data that's available to us at that time.

Q And when you are using this technology, whether it be the cell site location information or Google information or GPS information, what knowledge, skills and abilities are required of you in order to be able to analyze that?

A Knowledge of the records and how these records come to be. And that's where Cell Cos or cellular providers provide instruction of how these records are generated. Knowledge of the towers and an understanding of how radio frequencies work. How does a phone interact with a tower? How does a phone interact with a GPS sensor or a Wi-Fi sensor and overall how these things work in order to generate these records which then we can take and plot on a map.

Q Turning specifically to Google, have you prior to this

case, have you previously worked with Google location data?

A Yes, I have. Approximately 18 cases I've worked with Google location data from various different cases.

Q Have they all been cases involving Henrico County or other jurisdictions as well?

A Other jurisdictions as well.

Q Have you used historical records such as Google or cell site in order to exclude suspects as well as figure out where they are?

A I haven't personally done that but members of the CAST team have used information from cell site to exonerate subjects, yes.

Q What kind of records do you look at in order to conduct your cell site analysis?

A I look at the records that are provided from the provider. And in this case it would be the Google records that are reviewed. And Google's records already provide a latitude and longitude, a coordinate of where they estimate that mobile device to be at that time.

Q So when you get the records from Google, what is your process, what do you do?

A I look at the records and the records are coded in UTC time, Universal Time. So I adjust those records to be in the local time zone. And in this case, I believe it was Eastern Daylight Time. So we make that conversion so that we're

looking at the accurate time of where that device was when the records, or according to the records. I then take that information and two pieces on there or three pieces, the type or the source of that record and that could be one of many things. It could be from a GPS sensor. It could be from a Wi-Fi sensor. It could be from a cellular tower sensor. Or it could be unknown. I take the coordinates and then I take that accuracy radius that they give us and I plot that information on a map so we can see where Google believes that phone was, their best estimate.

Q How do you plot that on a map?

A I use a variety of tools. What I need to do is convert it into what we call keyhole markup language, it's KML and that's the language that Google Earth understands in order to import this data. So I have a process to convert that into the correct format for KML. And then I load it into Google Earth so I can view all of these points on a map.

MS. ULMER: Your Honor, at this time, we are asking that Agent D'Errico be an expert in the field of historical cell site data and location data analysis at this time.

THE COURT: I'm sorry, historical cell site data?

MS. ULMER: And location data analysis.

THE COURT: Do you care to voir dire Special Agent D'Errico, Mr. Mikula?

MR. MIKULA: With regard to the location service expert or service expertise, yes, sir.

THE COURT: All right.

VOIR DIRE EXAMINATION

BY MR. MIKULA:

Q You've never had any specified training from a Google developer or engineer, have you?

A Not specifically from Google.

Q So you're not privy to their algorithms or digital formula and how they create the data that you're given, correct?

A I am not privy to the exact algorithm as it is a trade secret to them. However, based on the data that is collected from the sensor from the phone, we can make some estimations based on academic papers as to what techniques they may be using.

Q So you can see it as an approximation?

A It is an approximation, that's correct.

Q And so you're not aware of the margin of error for the Google location services at all?

A Other than we have conducted some testing where we have tested the accuracy of that information. We do not have a precise number to tell you for an error rate. But I can show you in two slides some of the testing we have done to

determine the approximate location of, the approximation of Google's estimation versus the actual location where we were when we were testing.

Q And so have you been to any seminars or any other continuing education that's been presented from a Google representative?

A Not directly from a Google representative, no.

Q Okay, so essentially what you're saying is, is you received this data from Google, you analyze it based on your training and expertise as a cell site expert and your other credentials and then you plot it using the Google Earth application as well as other methods of software, is that fair to say?

A That's correct, yes.

MR. MIKULA: Okay, nothing further.

THE COURT: Do you care to be heard on the request for –

MR. MIKULA: Well, I have no problem stipulating his credentials as a digital expert, a forensic expert or a cell site or a cell data expert. The Google locations qualification, Judge, I do have concern for because it's kind of part and parcel with what our argument here is today is that he is certainly somebody who is qualified in a lot of areas but with regard to being an expert and opining as to the reliability of

Google's information, he has no background in that information. He doesn't know the DNA. He doesn't know the foundation of Google and certainly there are other ways in which the Commonwealth can satisfy reliability through other evidence but I don't think he's qualified to be a Google expert in this Court's eyes.

THE COURT: All right, at this time the Court will receive Special Agent Jeremy D'Errico as an expert in historical cell site data and location data analysis based upon his testimony and the cross examination by defense counsel. The Court notes the exception to the Court's ruling by counsel for the Defendant. Proceed.

FURTHER DIRECT EXAMINATION

BY MS. ULMER:

Q You already touched on this a little bit but based on your training and experience and in viewing academic papers, can you tell us how Google can determine the approximate location of a device?

A Yes. There are several ways that Google can do that. And that's tied to the source column that I was speaking about in the records before. So the first way and the way that's probably most accurate for outdoors would be using the GPS, the Global Positioning System sensor in the phone. And Google is constantly collecting information from phones. And

they admit to such and documentation both on their website and marketing material and in other locations. So Google is collecting this information and GPS is very accurate when outdoors. Indoors there is some reliability issues with it but Google doesn't collect just GPS. It also collects other wireless signals in the area. So in the case of a Wi-Fi source, Google is collecting all of the Wi-Fi access points that we may have in our house or a business to try to identify where it is. And Google collects information on a normal basis of, you know, from our phones, from every Android phone that has location services turned on. It's collecting a GPS coordinate and the Wi-Fi that's around the area. So that when it gets into a situation where a GPS signal might not be turned on on the phone, because GPS is very expensive as far as resources, it drains the battery faster than Wi-Fi would, Google has reference data so they can say well I've seen these four Wi-Fi access points before at this signal strength and last time I saw them, this was the GPS coordinate of the phone that saw it at those similar strengths. So I believe that the coordinate or the estimation of this phone would be in this area. And that's accurate because Wi-Fi has a limited distance in which it can actually broadcast out. Approximately 250 meters outside on a perfect, under perfect conditions is about the range that Wi-Fi can broadcast. Other sensors are less but indoors and most access residentially are indoors, a paper has said that it's

about seventy meters of accuracy. So Google knows that these signals degrade over time to a point where a phone can't see that signal. So if that phone is seeing that Wi-Fi signal, that means it's in the immediate vicinity of that Wi-Fi access point. And Google has previously collected information on where Wi-Fi access points are located across the entire world. It's a huge industry to collect that type of data and the location data services market. And research on this topic goes back way past 2006. It's not really a new topic. We've had radio frequency research done for years at this point.

Our third classification of data would be cellular and that's through cell towers. So if they can't get a fix on a GPS signal, if they can't get a fix on Wi-Fi signals, it's going to fall back to the cellular towers. And as you may know, the cellular towers have a much larger span than a Wi-Fi access point. And cellular towers can reach out a mile or so if not more depending on how the network has set up those cellular towers. So Google can fall back on that information saying well at least I know that this phone was in this vicinity of this cellular tower and can draw say a mile radius around that tower.

Q You made a lot of statements about what you believe Google does, how do you know this, what is your knowledge about that?

A I've done a bunch of research on Google, on

documents that Google has provided themselves, on documents that other researchers have provided and documented in papers. And I also understand other tests that have been conducted on Android phones to understand what type of data is flowing from the phone up to Google in order to make these decisions on the location services.

Q And you already kind of hinted at this a little bit, but is the field of determining where a mobile device is based on radio signals new?

A It is not new at all. CAST has been doing this type of work since 2006. The unit was formed in 2010 to formalize it but cellular providers have been collecting this type of information to troubleshoot their networks pretty much since instantiation of cell phones. And they need this information to be able to operate their network, to run diagnostics on their network and to make sure that their customers are being served. They are profit seeking and if they are not properly serving their customers, they are not making a profit, which means they would not survive. So they have much motivation to make sure they know where their customers are while making phone calls.

Q So can you determine the approximate location of a mobile device by using the location history data?

A Yes, we can.

Q Okay and that's by using all the different points that

you described, Wi-Fi, GPS and cell tower?

A That's correct. And we try not to rely on any single one point. But we try to take multiple points and multiple pieces of data into consideration in making a determination of where the approximate location of that phone.

Q And did you complete that analysis for this case that we're here for today?

A Yes, I did.

Q And typically were you asked to review location data for a Google account that was Roland.Anderson1907@Gmail.com?

A Yes, I was.

Q And in doing that analysis, did you prepare this PowerPoint presentation we're about to look at?

A I did, yes.

Q Speaking about Google, can you give us a general overview of Google as a company?

A Yeah, Google is a subsidiary of Alphabet. And it is, I believe, it is number three or four, the number three or four highest trading company on the stock exchange. It depends on which day you look. But their 2017 revenues were $110 billion and of that $110 billion, $95 billion of it was from advertising revenue. Their main source of income is advertising. And the same with Q1 to Q3 of 2018. $97 billion of revenue with $83 billion of it coming from advertising.

Google provides a number of products. The notable ones here might be the search engine Google.com, their email program Gmail.com, their Google Maps that is used to, you know, provide directions or navigation, their Android operating system, which is one of the top two operating systems for mobile phones. And then of course advertising, all the ads that we see on Google.com or in our emails or other on their mobile phones as well.

Q And to give all these products, they have to have a privacy policy, are you familiar with Google privacy policies?

A Yes, I am and they've had several privacy policies over the years.

Q Do they discuss location data in their privacy policies?

A They do and they started discussing location data in their privacy policy back in 2009, again, nothing that's new in this field.

Q Specifically do they talk eventually about Wi-Fi location data in their privacy policy?

A They do. In 2012, they modified their privacy policy to specifically include that they may receive from your phone nearby Wi-Fi access points and cell towers.

Q And do they continue to update their privacy policies?

A They do. They've updated it, they've updated the

location portion of it three times since the current policy.

Q And do those privacy policies continue to indicate Wi-Fi access point and cell towers as well?

A Yes, they do.

Q And is this a current privacy policy?

A This is a portion of it dealing with the location information.

MS. ULMER: This is slide four for the record.

BY MS. ULMER:

Q And I believe on slide four you've highlighted a particular portion, what is that portion?

A I did. So when you hover over the fourth point on the bottom left, the information about things in that device, I'm sorry, information about things near your device, such as Wi-Fi access points, cell towers and Bluetooth enabled devices. If you click on that link, you'll see that panel on the right side that explains a little bit more the information about things near your device. And specifically, I've highlighted the other sensors that Google says that it's going to collect such as information from accelerometers or nearby cell towers or Wi-Fi access points and specifically the MAC address or the Machine Access Code address and signal strength of that Wi-Fi access point.

Q And when you were talking earlier about the accuracy of Wi-Fi points, you were talking about signal strength, is that what a MAC address is?

A The MAC address is the unique identifier for the Wi-Fi access point. So it's kind of a like a telephone number for that device. The signal strength would be, you know, how loud and how clear is that signal being received.

Q Turning to the next slide, Google itself talks about and categorizes locations in two different categories, correct?

A It does. Google says that it's going to collect information on implicit location information or explicit location information. And implicit location information would be similar to, you know, actually I'll read their example. If you type in Eiffel Tower, we, Google, infers that you may like to see information for places near Paris and then we can use that to provide recommendations about those local places to you. So based on your search history and what you're searching, they're inferring in where you may be or the information that you were trying to see.

Q And what about explicit location information?

A Explicit location information is collecting information but from the sensors of your phone; so from the GPS sensor in your phone, from the Wi-Fi sensors and the accelerometer and gyroscope that are all built into modern day smart phones.

Q Going to slide six, what does Google say location

history does?

A Location history will include information that Google receives from location reporting, which is a device level setting that allows your device to send location data back to Google for use in location history. Essentially what it's saying is, it's determining your location history from the information that you are allowing your phone to send back to Google. And that's an option that you can turn on or off on your Android device.

Q And why would Google want to use location history data?

A Location history data is good for ad revenue. It allows their ad subscribers to target individuals in a certain area. For example, and this is a made up example but maybe PetSmart would like to target customers that are going to Petco, a competitor. They can set up an area that they would like to send a five dollar coupon to, to anybody approaching a Petco store. And the same thing, you know, they could also send a five dollar coupon to anybody approaching a PetSmart store. But they would not send that five dollar coupon to somebody say approaching a Walmart that is nowhere near a Petco or a PetSmart. It allows them to really focus in location-wise on where they want to send that advertisement. And with advertisement revenue being such a large portion of Google's revenue, they have a huge incentive to get this right, this

location correct.

Q And based on your knowledge, do they tell prospective buyers of Google advertising that they can target a particular location? Is that something that they advertise as being a service?

A They do. As part of their Google Ads service, which you can subscribe to and start pushing out ads, one of the categories of ads is a radius around a location. So they are saying that it allows you to choose to show your ads to customers within a certain distance from your business rather than choosing individual cities or regions or countries.

Q That was the example you were giving us of Petco and PetSmart?

A It was.

Q For advertising?

A Correct.

Q And in order to use radius advertising, the Google information, location information must be accurate?

A Correct, that's correct.

MR. MIKULA: Objection.

THE COURT: State your objection, please.

MR. MIKULA: I think to assume that it's accurate.

THE COURT: It calls for speculation.

MR. MIKULA: I would say so.

THE COURT: All right, objection sustained on that question.

MS. ULMER: I'll move on.

BY MS. ULMER:

Q Moving on to slide eight, why else would Google want to use location data?

A Google has their Google Maps platform where they use web services. And this is where Google can allow other companies or other applications to use their geolocation services. And in this advertisement for their geolocation with Google Maps, Google claims that they have the largest network of Wi-Fi points and cell IDs to ensure coverage anywhere on the Earth and that they are consistently updating through crowdsourcing from billions of Androids phone. No GPS is required in order to use their crowdsourcing location. And they also make a claim on their accuracy of their geolocation. The claim is, you know, advanced positioning algorithms deliver typical accuracies of ten to twenty meters and excel and problematic indoor and urban environments where GPS struggles. Perfect for IOT, which is internet of things, asset tracking, wearables and compliance.

Q We've already touched on this a little bit but how can the location be determined?

A The location can be determined using various

sensors on the smart phone. I listed a few of them, GPS, Wi-Fi, cellular, Bluetooth and those cover the radio frequency or the radio spectrum sensors. Then you have accelerometers and gyroscopes that determine if the phone is moving or how the phone is positioned. If it is positioned north, south, east, west, you know, on a tilt. A barometer that helps Google determine which floor in a building that you may be in. And then other user provided information such as directions from one place to another to determine approximate location.

Q And how do you know that Google uses these different sensors?

A Google has listed them in their various privacy policies and I believe we saw most of them in previous policies.

Q Turning back the next slide, specifically GPS, how is that location collected through the GPS sensors?

A There is a GPS receiver chip on all modern, most modern smart phones. And that GPS chip is listening to radio broadcasts from, you know, I believe it's 32 different satellites that the U.S. military has put into orbit. And Google needs or the phone needs about four of them to come up with a precise location of where that receiver or that phone may be. It's very accurate and very precise, especially outdoors. But it does have some downfalls. Specifically, what we call urban canyons or big cities where it's hard to see blue sky above you that does interfere with those radio signals. And the way that it

determines its location from those radio signals is that one of the elements of messaging in that radio signal is the precise time that that signal was sent. And that GPS receiver understands the orbit that that satellite is in and can calculate the distance that that signal needed to travel from that satellite to that receiver and the amount of time that it took to transmit that signal. And based on that information and signals from three other satellites, it can determine a precise location of where that receiver is.

Q How do you know how the GPS works?

A Based off of research papers that are published in academia and documentation from GPS.gov, which is the governing body for GPS in the U.S.

Q Do you get training in GPS?

A We have discussed it. I wouldn't call it explicit training in it. It's more research that I've conducted.

Q Research on your own. Turning now to Wi-Fi, how exactly does Wi-Fi work in terms of position of a cell?

A There is multiple ways that you can use Wi-Fi access points in order to determine positioning. And a lot of this research was done back in 2006, 2008 when they really started tackling alternative ways to determine location other than GPS. In particular, most of the research is for indoor use to determine which particular room or which particular area in a building that you may be. And that's in an area where there

is many, many Wi-Fi access points crammed into a small area so that you have a really good understanding. There's also been papers about using Wi-Fi in the outdoors and particularly studies walking down city streets because of the limitations of GPS and how they can determine locations from multiple Wi-Fi access points.

And the three techniques that I pulled out here are cell identity, which is probably the least accurate of the three. And that is essentially using a single Wi-Fi access point and looking at the signal strength from that Wi-Fi access point and then translating that into an approximate distance. So of course, if we don't see that Wi-Fi access point, we know that we're nowhere near that Wi-Fi access point. But if we see that Wi-Fi access point, we know that we're at least in proximity of it.

And as we mentioned before, Google does a lot of crowdsourcing and a lot of collection of where Wi-Fi access points are. So they have a huge database of the approximate locations of Wi-Fi access points. In fact, they have mine at home and they most likely have everybody's here, the location of their Wi-Fi access points because they've collected that through crowdsourcing or driving their Google street cars through the streets. So cell identity, they can't tell you a direction from that access point, it just knows that you're in the vicinity of that Wi-Fi access point.

Trilateration uses multiple Wi-Fi access points. Similar to how GPS measures the distance, trilateration is trying to measure the distance based on the signal strength of multiple Wi-Fi access points and knowing where those Wi-Fi access points are. So what you can do is, I drew three Wi-Fi access points out there in blue, green and red. And based on a signal strength, we can calculate a distance from each of those Wi-Fi access points. And if I draw a circle around the Wi-Fi access point from that, of that distance correlating to that signal strength, I can see that all three circles intersect in one point and that point is the believed, the estimated location of where that cell phone is located. Because it can see all three of those access points and it can measure the signal strength from all three of those access points. And that calculation would put it in that area. Now that again requires an exact location of where that Wi-Fi access point is.

But there is a third method that does not require the exact location and that's called fingerprinting. And fingerprinting, the way that it works is mainly through the crowdsourcing platform. So again, our phones, the Android phones are constantly collecting GPS coordinates when available Wi-Fi access points and their signal strength. And Google collects all that information and puts it into a database and then can run an algorithm when Google receives only Wi-Fi access points. It can compare that signal strength of the Wi-

Fi access points of this device with an unknown location has, query its database using a K nearest neighbor algorithm or some other statistical algorithm.

THE COURT: I'm sorry?

WITNESS D'ERRICO: K nearest neighbor. It's a statistical algorithm that helps you determine when you don't have an exact match where that may be.

THE COURT: Based upon where other people have been, historical data?

WITNESS D'ERRICO: Exactly, that's exactly right. Historical data from other cell phones that have been in that area that have collected data for Google. And it compares this unknown location that is seeing three or more Wi-Fi access points to all this data that it's collected and looking for somebody that has seen those three Wi-Fi access points at similar strengths and then looking at what their GPS coordinates were at that time. And they can determine an approximate location of where that phone was. And that's called fingerprinting. And you don't necessarily need to know the exact locations down to the centimeter of where that Wi-Fi access point is. All you're comparing are known Wi-Fi access points and the signal strength received by that device. And this data is collected billions of times a day through anybody that has the location services turned on on their Android

phone or uses Google's apps on an iPhone.

BY MS. ULMER:

Q So you mentioned the range of a Wi-Fi signal when it's outdoors, do you know what the Wi-Fi signal range is if someone's device is indoors?

A It's approximately seventy meters. And that again is very, I think it's very generous. You know, if you walk outside your house with your phone on Wi-Fi, it's going to disconnect from your Wi-Fi shortly thereafter walking outdoors. It could be a few meters away but I don't think you're going to get seventy meters away from your house. That's almost, that's three-quarters of a football field. I don't think you're going to get that far before switching off Wi-Fi. At least I can't at my house.

MR. MIKULA: I'm going to object. He said seventy feet, or he said seventy meters. I think that answers the question. When you look at his presentation where I think on page 11 of 46, we can move along. My objection just is she asked the question about the distance, he said seventy. I think that answers the question.

THE COURT: Do you object to seventy meters being approximately three-quarters of a football field?

MR. MIKULA: I don't object to that. Just that –

THE COURT: The generosity of the –

MR. MIKULA: Judge, my position is, is that he, she's certainly asking questions and he's answering those questions and going on and I'm just trying to move things along. So I think that he answered the question she asked.

THE COURT: I do as well. Objection is overruled.

MR. MIKULA: Yes, sir.

BY MS. ULMER:

Q You've already mentioned but for data location, how does Google collect that data?

A Google collects it mainly two different ways. One is with their Google street cars and the second way –

Q This is a picture of a Google street car?

A That is a picture from Google's website of a Google street car complete with the cameras on top. And the other way is through the Android phone and the Google Apps platform, which I believe we discussed.

Q Can you please explain what a geolocation API is?

A Yes, the geolocation API is an application programmer interface. This allows the developer of an application to use Google services in order to determine the approximate or the estimated location of that phone. So Google will ask for certain parameters to be sent to Google in a particular format and then Google will send a response back in

a particular format.

Q Why would you want to know this information?

A Applications want to know where the phones are. So a lot of applications that I've used in the past such as Panera Bread, they want to give you the opportunity to locate the nearest Panera Bread and they do that by determining your location and they can use Google services to do that if they don't have a program to do that on their own.

Q And turning to slide fourteen, what is this?

A This is the Wi-Fi access point object of this geolocation API. And this is the information that Google is requesting that you provide when querying the geolocation services or the location services when you only have Wi-Fi access points. So it's asking for a MAC address, which is that unique identifier for that access point, the signal strength, the age of when you saw it, so how long ago you saw this. Is this today, is it yesterday? Because we know access points do move. And then the signal to noise ratio. And some of these are optional. The only one that's actually required is the MAC address.

Q And when Google responds, what do you receive?

A In response back, we receive a location, which contains a latitude and a longitude and then an accuracy in meters of where they believe this device may lie.

Q Turning now to Google geolocation, you've already

talked about the background and the methodology a little bit but is this, did you guys conduct your own analysis basically or observations of Google location data?

A I did. I went out and wanted to compare our actual locations with the Google estimates that they provided using this geolocation API.

Q Can you explain the methodology to the Court how you did that?

A Yes, absolutely. So essentially, I took a phone with me to determine my actual location and I recorded the coordinates of my actual locations. And then I used a computer and software that was not connected to the network so that Google could not receive any information in advance of this request and I scanned for all of the Wi-Fi access points that were visible to this computer. I collected the MAC addresses and the signal strength as well as some other information. And then I provided this information to Google through their geolocation API and received the coordinates back from Google of Googles estimated location for these points.

Q As turning to slide eighteen, you made multiple observations, is that correct?

A That's correct.

Q Can you please explain slide eighteen observation one?

A This is an observation outside the Henrico County Administration Building. The red dot on that chart is my actual location when I conducted the observation. I collected the information, the Wi-Fi information sent it up to Google at a later date and Google returned back to me that the point was located at the green marker and that the accuracy radius is illustrated in the green circle around the point.

Q So for observation one, was your observed location within the accuracy circle?

A Yes, it was. The observed, the actual distance between Google's estimated location and my actual location was 35 meters. And Google's accuracy was 57 meters, so well within the range.

Q Turning to observation two, could you please explain what happened in that situation?

A Yes, this was an observation outside the Henrico County Courthouse, pretty much right in front of the front doors illustrated by the red dot. And similar, I collected Wi-Fi information, sent it up to Google using the location API and they returned the position of the green marker with the radius of that circle. And in this case, Google was off. The actual distance was 69 meters. And Google estimated their accuracy would be 48 meters. But in this case, it still puts it at the Henrico County Courthouse. I know that I'm not at Hermitage High School, or Google doesn't estimate them at Hermitage

High School or even at the juvenile relations, which are the nearest buildings. It still sees it at the Henrico County Courthouse.

Q Turning to observation three, could you please explain where you are at that time?

A This time I'm at Parham Doctor's Hospital, down the street from here. The red dot again is where I am. The green dot is Google's estimated location and the ring is Google's accuracy. At this point, the distance between Google's estimate and my location was fifteen meters and their accuracy was up to 74 meters.

Q So were you standing within the Google circle of accuracy for observation three?

A Yes, I was.

Q Okay, going to observation four, could you please explain where you were at that time?

A This is an observation on Winchmere Court, which I wanted to make observations in both townhomes and apartment complexes, public buildings and public areas to get a variety of estimates. So this is an apartment complex down the street from, not too far from here, about a mile or so from here. And, you know, again, observation of the red dot, Google returns the green dot and the ring of accuracy is 130 meters. We turned about to be 42 meters from Google's actual estimate, or Google's estimate, excuse me.

Q So within the Google accuracy circle?
A Yes.
Q For observation four, are you still in an apartment complex?
A Yes, this is.
Q Okay and is it the same apartment complex?
A It's across Schrader Road but related complex.
Q Can you please explain what happened in observation five?
A Observation five, we collected Wi-Fi. My position was at the red dot and the green estimated distance away was about twelve meters from Google, with an accuracy radius of 39 meters.
Q Again you were within the accuracy circle?
A Yes, we were.
Q And observation six, could you please explain where you are in observation six?
A On Channing Green Court in front of the building marked, between the buildings marked 8401 and 8404 indicated by the red dot. Google provided the estimated location, approximately nineteen meters away.
Q And is that within the Google accuracy circle?
A Yes, it is.
Q Turning to observation seven, where are you now?
A I'm at Shannon Green Court, which are townhomes,

not too far from my last observation. In fact, it's probably about, just looking at the scale on the map, it's probably a little over a hundred meters away, probably yeah, just a little under a hundred meters. And this point has put me, Google's estimate was nine meters away from my actual location and within the circle of accuracy.

Q Observation eight, are you still in the apartment complex or what kind of area are you now?

A These are townhomes with, on Green Run Drive. And I'm actually on the street in between the two complexes. I'm on the right side of the street as you can see from the red dot. Google provided an estimated accuracy or an estimated distance 21 meters away from my location. And it was inside the 113 meter ring of Google accuracy.

Q Turning to observation nine, what kind of area are you in now?

A Again some townhomes over on Coachford Court. The red dot indicates my location. Google places its estimate 46 meters away from me and it's within the 67 meters that Google has provided for its accuracy.

Q Observation ten, are you still in the townhomes or where are you located?

A I am. I'm actually only a few meters away from where I was. So my last observation nine, if you look at my red dot and follow that road to the left, I am near the intersection

of it's Old West Drive and Coachford Court. I moved just to the other side of that small little townhouse street. And I received an estimated location that was 54 meters away but again inside the 102 meters that Google has provided.

Q Observation eleven, where are you?

A I'm at the Kroger that's at 9000 Staples Mill Road at the intersection of Hungary Spring Road and Staples Mill Road.

Q And again, are you at the red dot?

A I am. I'm at the red dot in the center of the parking lot, trying to be further away from Wi-Fi access points.

Q Okay and so what happened in this instance?

A Google provided an estimated distance that was 71 meters away from my location outside of Google's accuracy radius of 58 but still places me inside that Kroger parking lot.

Q How many meters was it off, Google accuracy versus where you are?

A The accuracy off doing the quick math, thirteen meters.

Q Yes.

THE COURT: Would you mind if I asked a question?

MS. ULMER: Yes.

THE COURT: So for the difference between observation nine and ten you've indicated that it's a short distance that you moved?

WITNESS D'ERRICO: That's correct.

THE COURT: But the range of accuracy went from 67 meters to 102 meters, is that because of the different Wi-Fi strengths, what increases the accuracy radius?

WITNESS D'ERRICO: I did not compare to see if I collected the same Wi-Fi access points from both location nine and ten to see if they saw the same Wi-Fi access points. And again, I don't know exactly how Google comes up with their estimates. All I'm doing here is testing pretty much in a black box, providing it inputs and seeing where it sees that I am. And based off of those tests, I can still see it provides different accuracy radiuses but still in the same general area of where my observation was.

THE COURT: Okay.

BY MS. ULMER:

Q Okay, going to observation twelve now, which is slide 29, are you still at the Kroger?

A I am at the Kroger and I'm about I think it's about five parking spaces away from the Marketplace side of the Kroger, near Marketplace door.

Q And where does Google think you are?

A Google places the estimate location, estimated location inside the Kroger or within the footprint of the Kroger, which is 57 meters away from where I actually was and it's

outside of Google's accuracy ring.

Q By how much outside are you from the Google accuracy?

A It's about 15 meters, doing the math on the fly. But again, puts me in the Kroger parking lot, in that Kroger area.

Q For observation thirteen, where are you?

A I'm in the Kroger parking lot, this time near the pharmacy door, which is just on the other side of the Kroger building. And this time Google provides me an estimate and this was the largest difference that I saw in my testing and it believed that I was 253 meters away towards the top of the shopping center versus near the Kroger door.

Q And can I ask you to do some quick math about the difference in the distance?

A Yes. That looks like it's 190 meters away.

Q And did you compile this into a table, is that on slide 31?

A I did. That's the table of the locations, the latitude and longitude for each of the points and then it did some calculations here, too. So the actual distance away, which we saw in the slides, the number of BSS IDs, that's the base station identifier, that MAC address. So this is how many MAC addresses I submitted to Google for each location. And then the maximum RSSI, which is the received signal strength indicator, so the strength of the signal. And then I calculated a

maximum, a minimum and an average. And the way to read those received signal strength indicators, you'll see that they are all negative numbers. The closer to zero, the stronger the signal. So for example, picking out two signals on here, you know, I'll just take the first line of course the maximum is larger than the minimum, so -58 is a stronger signal than -90 on that first line.

Q And again, what does that mean to you?

A That means, you know, for those signal strengths that are higher, it is much likelier that the phone is nearer to that device. So you can use that fingerprinting algorithm or any of the other algorithms up there to determine the approximate location of that phone.

Q In addition to the tests that you yourself conducted and that we've just gone through, are you aware of accurate papers that have also written about Wi-Fi locations themselves?

A Yes, I am. And some of those papers are listed for you.

Q And you, of course, did your own observations but are you aware of any other studies that have been done by other entities?

A Yes, I am.

Q And what are those?

A There was a study conducted by Oracle, where they

developed a system to, it's called a man in the middle. They are looking at the network traffic that's actually coming off of the telephones and that is going to Google so they can determine the exact information that is being transmitted to Google in order to determine the location of the phone.

Q And so as part of that study, what are they trying to, what were their findings and what are they trying to do?

A Their study was mainly to, it started off to determine if there was any privacy implications with smart phones. And they were looking at data and they came across this data as they were conducting their research.

Q And what was the finding of the study?

A That the information that came off the phone –

MR. MIKULA: I'm going to object. This is hearsay, Judge. I think if he can provide the actual study and submit that into evidence by way of witness, then they can but that's hearsay.

THE COURT: Do you care to be heard on it?

MS. ULMER: Yes, sir. Judge, I believe that as an expert he can rely on other studies and other knowledge so he can testify as to what his knowledge of other studies are and he can, of course, be cross examined on that but it is something that he is aware of as an expert and he can testify as to what he knows.

THE COURT: I believe that he can testify based upon what the data showed but not what the opinion of the person who authored the data is. So I don't believe that this witness is testifying as to what the opinion is but basically what the data showed. So I overrule the objection.

BY MS. ULMER:

Q Can you please tell us what the data showed?

A The data showed similar to what the geolocation API contained. It showed information such as Wi-Fi access point, BSSIDs or MAC addresses and signal strengths being transmitted to Google as well as the GPS coordinates, part of their collection platform. And in return Google was sending back an estimated latitude and longitude and estimate radius for those coordinates.

Q Was the data collected by the study similar to the data that they later received from Google?

A Yes, it was.

Q Turning now to, you've already mentioned that you testified three times about Google location services in Henrico County, was that in the Commonwealth versus Denise and LaToya Gay cases?

A Yes, it was.

Q All right and can you please explain to the Court a little bit of the background of that case and what you were

asked to do?

A Yes.

MR. MIKULA: I'm going to object to the relevance as to what happened in another case. I don't know how that's applicable here in terms of the reliability of this information. It's a separate case, a separate fact pattern, I don't know the relevance.

THE COURT: Does it make a difference as to what he did and he was determined to be an expert in those cases and you'd stipulate to that Mr. Mikula?

MR. MIKULA: Well, I stipulated as to his expertise with regard to the cell phone data.

THE COURT: Do you concur that he was determined to be an expert in those previous cases?

MR. MIKULA: I don't have any objection to that.

THE COURT: And he testified as an expert in those cases, do you agree with me?

MR. MIKULA: I agree with that, sir.

THE COURT: Okay, so what is it that you are asking Special Agent D'Errico to testify to as to the previous cases?

MS. ULMER: In those previous cases, your Honor, the reason why we are here is whether or not this information is inherently unreliable or if it can be presented to the Jury.

This case in particular, what I'm hoping to show through Agent D'Errico is going to whether or not the Google information is reliable and what he knows and I believe that is a direct issue in this case.

THE COURT: Well, doesn't that go to the weight of the evidence? Isn't it basically that he testified and the finder of fact made its determination based upon the testimony of the witnesses?

MS. ULMER: Well and they did ultimately, I don't know exactly, you know, obviously was not in the Jury Room, Judge, to know what weight they gave it. But I think it's relevant for your Honor to see that in another case with Google location services, the accuracy of that information that was provided it has great weight onto the accuracy of the information before your Honor today in regards to Mr. Anderson's case.

THE COURT: But everything goes to the weight.

MS. ULMER: Well, Judge, in the Denise and Latoya Gay case there is specific corroborations to the Google location information that was available in the Gay case but was not necessarily available in the case before your Honor. So I think it is important for the Court to see that in another case in Henrico where we have the exact same type of information how it can be corroborated and how it was corroborated in that case and thus the information is reliable in this case and

should be admitted into evidence.

THE COURT: What I believe I'm hearing you say is that the Special Agent testified to Google location services in these previous cases.

MS. ULMER: Yes.

THE COURT: And there was independent evidence to show the corroboration?

MS. ULMER: Yes, sir.

THE COURT: So why does he need to go through all these slides as opposed to say it was my opinion that it was located here and then the evidence that was independent showed that it was either exactly or close by or in the same town or anything like that, why do we need to go through these slides?

MS. ULMER: Well, Judge, if we're willing to have the Defense stipulate that it was extremely accurate, then I have no issue with that. However, if he is not willing to stipulate, I'd rather go through the slides to show that when Google says that, for instance, Denise Gay is at one particular location and something else shows that at that exact same time she was at that location. If Mr. Mikula is willing to stipulate that the evidence was corroborated that the Google location was corroborated exactly, then I have no issue. I don't need to go through the slides.

THE COURT: Does this Special Agent, is he able to

testify as to the corroborated testimony?

MS. ULMER: Yes, sir. That's what he's testified to in the Gay case.

THE COURT: Why can't he, then do you agree Mr. Mikula he could say my Google location services had this and that the corroboration testimony had the location dead on, outside the zone or anything like that? I just don't know that I need to, we need to go through these slides to get to that point. I think that, do you agree with that Mr. Mikula?

MR. MIKULA: I don't know if, I mean I think that he, they are certainly doing what they need to do in terms of showing how it is reliable and it's our burden, well not our burden but it's our duty to certainly cross on issues that's already been presented to the Court. How, we're left to assume a lot in terms of what happens in a separate case and so –

THE COURT: Let me think about it this way. If we hold on this, if on cross examination it gets to that issue, then on redirect you can ask the Special Agent more particular questions. Fair enough?

MR. MIKULA: That's fine.

MS. ULMER: Yes, Judge.

THE COURT: Okay.

MS. ULMER: Judge, am I allowed to ask a general question about the Gay case?

THE COURT: It depends on what the general

question is.

MS. ULMER: Okay.

THE COURT: You can try.

BY MS. ULMER:

Q In the Denise and Latoya Gay cases, were you able to corroborate the Google location data you received with other evidence such as her bank statements?

A Yes, we were.

Q And that data from the Google location, the Google location data, was that accurate with what you saw in her bank statements of her location?

A Yes, it was. It provided the estimated location of where she was, which matched Google's estimation.

Q Okay, let's turn to slide 38.

THE COURT: May I ask one other question?

MS. ULMER: Yes, sir.

THE COURT: The Commonwealth has allegations that this Defendant was at certain locations, is that correct?

MS. ULMER: Yes, sir.

THE COURT: Has this Special Agent gone to those specific locations and done the independent analysis to determine whether or not that he's within or outside of the zone of accuracy?

MS. ULMER: Well, Judge, that's what we are getting to. He did not go back out with the cell device. However, similar to the Gay case, we have other evidence that will be presented to your Honor that corroborate the Google location data with where Mr. Anderson was.

BY MS. ULMER:

Q All right and the Roland Anderson case, approximately how many data points did you receive?

A 2,608 data points.

Q And what was the timeframe for those points?

A October 12th, 2017 from 8:01:24 p.m. to October 16, 2017 7:59:51 p.m. in Eastern Daylight Time.

Q And so that is when you converted from UTC to Eastern Daylight Time?

A That's correct, yes.

Q And we've already gone over the different fields that you received in that data. So turning exactly to slide 39, what does this slide show?

A Slide 39 shows the Google location points that Google provided between the time of 11:58 a.m. and 1:44 p.m. on October 15, 2017.

Q And what do the blue balloons mean?

A The blue markers indicate that the source of that data as marked by Google was Wi-Fi.

Q And what about the red ones?

A And the red balloon is GPS as provided by Google.

Q And what is this location?

A This location is, the general location is the Kings Point Apartments. The yellow marker indicates where Mr. Anderson's residence was in apartment B and the crime scene location in the same building in apartment H.

Q And so what does the slide mean to you?

A The slide indicates to me that the mobile device was at this apartment complex between the times of 11:58 a.m. and 1:44 p.m.

Q Turning to slide forty, what is this, is this Google location information you received?

A This is. Between the times of 10:22 a.m. to 10:37 a.m.

Q And again, what is the blue marker?

A The blue markers are Google location history data points marked with a Wi-Fi source.

Q And what about the green?

A And the green is Google location history records marked with a cellular source.

Q And what is the, you said the times are 10:22 a.m., where is the first point at 10:22 a.m.?

A The first point is near Mr. Anderson's residence, near the apartment complex.

Q And for the record, can you explain the travel and the timing of these different data points?

A Yes. So you can see in sequence the data points are moving up Laburnum Avenue and make a left turn, I'm not familiar exactly what that street is but it ultimately leads down to the Kroger. And in this case, you can see the green markers, the times are shaded a little darker and they are not included in the sequence because the error radiuses were nearly 1300 meters for that. So that point in particular would put that device in the 1299 meter radius circle, which doesn't really help with the accuracy of this information. So I added it for completeness but I'm relying on the Wi-Fi because they have a much smaller accuracy range.

Q What is the accuracy range?

A It's between 22 and 98 meters for each of those points.

THE COURT: And that's the blue?

WITNESS D'ERRICO: That's the blue points, correct.

BY MS. ULMER:

Q Were you able to corroborate this travel pattern using any other information provided to you by the Commonwealth?

A I was, yes.

Q And that is slide 41?

A That's correct.

Q What is that?

A This is an overlay of the Google information that we just saw on the last slide with the red marker or the red markers, which is RTT data, it's a tool that Verizon uses to determine the approximate location of phones. And in this case, we are looking at the victim's phone, the victim's phone records. So in this case, up near points three and four, there are two records provided by Verizon; one at 10:27:46 and one at 10:27:51 that indicated that the phone, that Google approximates the phone was located at that location inside the, it's difficult to see but it's kind of like a red band. In this example, it's pretty much directly next to the cell tower and the cell towers are illustrated by the red dots on the map, the small red dots with the wedges originating out. And that shows us our direction from a cell phone that Verizon believed that phone was positioned in at that time.

Q So are the, was the victim's phone and the Google location data similar?

A They are. They're actually in sequence all the way through.

Q Turning now to the Kroger itself, what was the information we received from Google?

A Between 10:37 a.m. and 10:47 a.m., Google provided these ten points. Two of them were GPS points. Eight of them were Wi-Fi points. And it provides that the phone was in the area of the Kroger between those times.

Q And there are blue balloons and then there is a red balloon. What is the red balloon there?

A The red balloon is the GPS as well as the rings around it illustrate the accuracy range for those GPS points. So that smaller circle in there represents six meters and the larger circle is 23 meters of accuracy for those GPS points.

MS. ULMER: Your Honor, at this time, the Commonwealth would like to admit three photos into evidence, which are from the Kroger surveillance for the purposes of the record. It shows Mr. Anderson entering at 10:39:28 and it shows him exiting at 10:47:49 and then that second photo of him exiting at that 10:47:51.

MR. MIKULA: We have previously stipulated.

THE COURT: Any objection?

MR. MIKULA: No, sir.

THE COURT: The photographs will be collectively Commonwealth's number Two.

NOTE: Commonwealth's Exhibit 2.

THE COURT: Before I forget, if we don't get to the issues having to do with the Gay case on cross, how are you going to have those slides that were not addressed redacted from the DVD that's been introduced into evidence?

MS. ULMER: Judge, I have a copy on my desktop of the presentation. I'm happy to go and delete whatever slides.

THE COURT: Any objection to that, Mr. Mikula?

MR. MIKULA: No, sir.

THE COURT: Okay.

MS. ULMER: Your Honor, as Commonwealth's Exhibit number Three, we'd like to enter into the record that ECO ATM receipt, which shows Mr. Anderson entering the victim's cell phone on October 14, 2017 at approximately 10:39:23 at the Kroger, Commonwealth's Exhibit number three.

THE COURT: Have you seen that as well, Mr. Mikula?

MR. MIKULA: I have.

THE COURT: Any objection?

MR. MIKULA: No objection to that.

THE COURT: Commonwealth's number three, without objection.

NOTE: Commonwealth's Exhibit 3.

BY MS. ULMER:

Q Did Google also send location information about a Tweeter Court address?

A Yes, it did, yes.

Q And if you could explain what is before us?

A Yes, the points mapped are between 1:30 a.m. and 3:51 a.m. on October 15th, 2017. And they put it, they put the phone in the vicinity of 6308 Tweeter Court in Richmond, Virginia.

Q And as part of your analysis, did you also analyze Mr. Anderson's cell phone?

A Yes, I did.

Q Did you find any text messages that corroborate Mr. Anderson being in that general location at that time?

A I did. I found two text messages on Mr. Anderson's phone. One sent from Mr. Anderson at about 1:14 a.m. and I apologize, let me explain the dates. This is directly from the Celebrite report. And Celebrite uses a European date format. So while it's marked 15/10/2017, it's actually October 15, 2017. The first message reads, I'm at yo crib. And he receives a message back from Keon, and Keon is the name that is in Mr. Anderson's phone that's associated with that telephone number that was texted to and from. At 1:23:59 a.m. saying, about to pull up in about five to seven.

Q On this slide, it looks like it says Keon Vaughn, how

did you come by that information?

A I used a public record search based on that telephone number to derive the name and address associated.

Q Where does Keon Vaughn live?

A 6308 Tweeter Court, Richmond, Virginia.

Q And in regards to the Google map itself where is 6308 Tweeter Court, Richmond, Virginia?

A It is where that arrow is pointing, which appears to be in the middle of many of the markers on there.

Q And the markers that are on there, are they both GPS and Wi-Fi markers?

A Yes, they are with the blue being the Wi-Fi and the red being the GPS.

Q In the Google location information that you were given, does it show a trip to Chippenham Hospital?

A Yes, it does.

Q And when was that?

A Between 3:51 a.m. and 4:03 a.m. on October 15, 2017.

MS. ULMER: Your Honor, at this time I'm going to take a pause from the presentation and play a previously stipulated jail call.

THE COURT: Any objection?

MR. MIKULA: No, sir.

THE COURT: All right.

NOTE: AN AUDIO RECORDING IS PLAYED BEFORE THE COURT.

MS. ULMER: Your Honor, the Commonwealth would like to admit the jail call as Commonwealth's Exhibit number four.

THE COURT: Any objection?

MR. MIKULA: No objection.

THE COURT: The jail call will be Commonwealth's number four.

NOTE: Commonwealth's Exhibit 4.

BY MS. ULMER:

Q Okay and going back to the Chippenham Hospital slide, slide 44, the Google location points, are they Wi-Fi, GPS or cell tower points?

A Eight of the points are from Wi-Fi and one of the points is from a cellular signal.

Q And finally, did you receive geolocation information regarding a Bradbury Road address?

A Yes, I did. I received Google location points in that vicinity yes.

Q And what type of points are those?
A It's a mix between GPS points and Wi-Fi points.
Q And do you know the owner of 8150 Bradbury Road?
A According to real estate records, it's Roland Anderson, different than the Defendant Roland Anderson.
Q Not Roland Anderson III, but another Roland Anderson?
A Correct.
Q And you mentioned multiple times throughout your report that and throughout the presentation that's it's based on academic, your knowledge with academic journals and other studies, have you listed all resources for his Honor?
A Yes, I have.
Q Okay and that is the next two slides?
A That's correct.

MS. ULMER: Your Honor, if I could have a brief moment. Judge, the Commonwealth would pass the witness.
THE COURT: Cross?

CROSS EXAMINATION
BY MR. MIKULA:
Q Remind me again of the pronunciation of your last name.

A D'Errico.

Q D'Errico. Mr. D'Errico, a few questions. In terms of the CAST presentation that you created, on page eight you had made comments regarding the accuracy. That information, now you created this presentation, is that correct?

A Yes, I did.

Q Okay, but you pulled some of this information from Google's website, is it fair to say?

A Yes, I did.

Q And the accuracy summary, that was derived from Google themselves, correct?

A If I could view the slide.

Q Page eight.

A Your Honor, I have a copy here if you don't mind.

THE COURT: Okay, page eight.

WITNESS D'ERRICO: And can you ask that question again, please?

THE COURT: Sure. On page eight, where it says accuracy, you took that from what Google gave you, is that the question? MR. MIKULA: That's my question.

THE COURT: Okay.

WITNESS D'ERRICO: That is correct. This is directly from a leaflet that Google uses as marketing material.

BY MR. MIKULA:

Q Okay and as part of that marketing material, you said that Google obviously is profit seeking, correct?

A Yes.

Q And a major source of that profit is advertising purposes, fair to say?

A Yes.

Q Okay. With regard to and you testified as well and you gave a hypothetical Petco versus PetSmart, do you remember that hypothetical?

A Yes, I do.

Q Okay and you said in some instances let's say if Petco gives, pays money to Google, they'll offer certain discounts so that people that are close to PetSmart will instead go to Petco or something to that effect, is that fair to say?

A That's fair, yes.

Q Okay, so you're basically saying that Google is willing to manipulate the consumer to come to a specific person?

A What I'm saying in that case is Google is willing to push out ads on behalf of their client. And Google is not determining the radius or where those ads are being pushed out to, Google's client is, PetSmart in that case.

Q Correct but my point is, is that Google will receive money from people and they will in a sense look at where their

location is, determine where potential client is and tell the client location that might be further or closer, is that fair to say?

A I'm sorry, I'm not understanding your question.

Q What I'm asking is, you said the hypothetical Petco versus PetSmart.

A Yes, sir.

Q Let's assume PetSmart is closer to a consumer. Petco is further away. But Petco pays Google money, will Google in your understanding and your background and expertise, will they tell a consumer to go to the further distance one if that person is paying them money?

A I don't know that Google tells them. Google has an ad platform and Google certainly pushes out ads on behalf of their clients. And what those ads contain, I don't believe that Google has full control. Of course, they have guidelines of what can be in those ads, but I don't know that they, that Google themselves are creating those ads rather than, in my example as I was discussing, the client can develop a radius or an area where they would like users targeted for those ads.

Q Okay. I'll move on. With regard to you said the history of obviously cell triangulation, Wi-Fi and GPS, that predates using Google to get that information, is that fair to say?

A Yes, it does.

Q Okay, so it's relatively recent that the FBI and other experts in the field have been using Google to generate this data?

A Recent, more recent than –

Q More recent than other ways in which to get the information that you've used previously?

A It is, yes.

Q And historically it was some, Google was used for purposes of a consumer, in other words my question is, is to your understanding Google is historically and has created, I should say this. Has Google historically been used as a person finder, a forensic tool or has that been a recent development?

A I don't know the first time that the FBI or any law enforcement agency approached Google. So I don't have that information. I can tell you that I've used it multiple times in the last year if not two years.

Q Okay, when is the first time you testified in a case using Google location services?

A December 2017.

Q Okay. And to your knowledge, Google has been using location services prior to December of 2017, is that correct?

A That's correct.

Q When did that first start?

A I don't know. As I mentioned in the presentation,

they added it to their privacy policy in 2009. I don't know exactly when they started using it, though.

Q So your testimony is you don't know when Google first used location services?

A I don't know the exact date, no I don't.

Q Okay. With regard to location services, you also testified it's tied in to not just Gmail but other applications in Google is that fair to say?

A That's correct, yes.

Q Okay and depending upon the type of let's say phone, is it built into let's say a Samsung Galaxy, versus you have to download it if you have an iPhone?

A Well, a Samsung phone typically runs the Android operating system. And this setting is in the Android operating system. The applications are used more so on the iPhone platform, which a user would have to download those applications such as Gmail or Google maps, do not natively come on an iPhone when you purchase it new from a store. Did that answer your question?

THE COURT: It's embedded in the Galaxy, in the Samsung phone but it's not embedded in the iPhone?

WITNESS D'ERRICO: That's correct. It's embedded in the operating system, the actual operating system. So there is no apps to download if you are using an Android based

phone, which Samsung creates an Android based phone. There is a setting to turn it off in the Android operating system. However, during the setup of those Android phones it asks if you want to collect this data and in my experience, I am in a rush to set up my new phone because I'm very excited and yes, yes, yes, yes, click through just about everything.

BY MR. MIKULA:

Q Okay, now you testified regarding the, I guess, the building blocks of Wi-Fi technology. And in that testimony you talked about the MAC address, do you recall that?

A Yes.

Q Okay and you identified the MAC address as the machine access control, is that correct?

A Yes.

Q Is it in fact called the media access control?

A You are correct, yes, I did misspeak there.

Q Okay.

MR. MIKULA: Regarding this Google data that I think has been previously marked and identified and moved into evidence as Commonwealth's One, do you have that able to be pulled up?

MS. ULMER: No.

MR. MIKULA: Okay. Judge, for demonstrative

purposes, I printed off the raw Google data that's been previously provided by the Commonwealth's Attorney's office and I can provide one to the witness as well.

THE COURT: Any objection?

MS. ULMER: No, sir, your Honor.

THE COURT: All right.

MR. MIKULA: And I'd like to pass one up to the Court as well.

THE COURT: Thank you. At this point in time it's just for demonstrative purposes?

MR. MIKULA: Yes, sir.

THE COURT: Not an exhibit?

MR. MIKULA: No, sir.

THE COURT: Okay.

MR. MIKULA: It's previously been moved in as an exhibit.

THE COURT: Is that part of the disk that was in?

MR. ACKLEY: I think it is.

MS. ULMER: It is the disk.

THE COURT: The disk is number one?

MR. MIKULA: Yes, sir.

THE COURT: Okay.

MR. MIKULA: Yes, sir.

BY MR. MIKULA:

Q Sir, can you please identify that set of documents, those pages you have in front of you?

A Yes, it appears to be a printed copy of the Google location history.

Q Okay and that is, you have 59 pages, is that correct?

A Yes, sir, I do.

Q Okay. There are a number of columns in this document is that correct?

A Yes, there are.

Q Okay, I'm going to ask you about each column and have you explain what it means. You had testified previously about the first column, which is UTC, correct?

A Yes, I have.

Q And remind me again of what UTC stands for?

A It's Universal Time Coordinated. It's not necessarily a time zone but it's a time that actually marks up with Greenwich Mean Time for purposes of time zone. So that we can shift time zones off of there.

Q Okay and the second and third columns, what are those?

A Column B and column C are marked latitude and longitude, which is the coordinates of Google's estimated location.

Q And that's a global positioning term is that fair to say, that those are global positioning terms?

A Yes, they are.

Q Okay and the fourth column, what is that?

A The fourth column, column D is marked display radius meters and that is Google's accuracy radius back to us.

Q Okay and for people that are not familiar with the metric system, how long is a meter in feet?

A It is just shy of three feet, so roughly equivalent to a yard, I don't have the exact –

Q Does it maybe is it 3.2 feet would you say, does that sound familiar?

A It may be.

THE COURT: About 39 inches or so?

MR. MIKULA: I think the Court can take judicial notice that a meter is 3.2 feet approximately.

THE COURT: There are less meters in a football field than there are yards?

MR. MIKULA: That's correct, yes, sir.

THE COURT: Okay.

BY MR. MIKULA:

Q And the next column, what is that?

A The next column, column E is the source column.

Q Okay and what's contained in the source column?

A In this document there are four different values in

that source column. It's Wi-Fi, GPS, cellular and unknown.

Q Okay and device tag, what is that?

A I don't have an official definition of what the device tag is. I'm unaware of what that column is.

Q You don't have, in terms of all your hours and experience in this type of field, you can't, you don't know what it is?

A No. I can guess what it is but I can't tell you with any certainty what it actually is.

THE COURT: Okay, would it be fair to say that for all the entries within the 59 pages the device tag is the same Mr. Mikula?

MR. MIKULA: Yes, sir.

THE COURT: It would have something to do with a device?

MR. MIKULA: I believe it identifies the device itself, yes, sir. But again that's –

WITNESS D'ERRICO: And I can offer that in other cases that device tag does not show up in any other case that I've worked. It is a different identifier for each set of data that I've analyzed.

MR. MIKULA: I'd ask that be stricken from the record. I didn't ask that.

THE COURT: Okay, we'll strike that.

MR. MIKULA: Thank you.

BY MR. MIKULA:

Q What is the last column please?

A The last column is the platform column and it describes the mobile device that was used as the source of this data.

Q Okay. Going to let's see, so if you take for instance columns B and C, which are marked as latitude and longitude and you can take those figures, those numerical, I guess, the numbers that are in B and C and you can plot a location point on a map, fair to say?

A Yes.

Q Okay and going back to column D that's marked as display radius in meters, is that fair to say?

A Yes, it is.

Q Okay, now when it says it's a radius, does it mean a distance from that point you would plot on a map, like a longitude and latitude to the outer edge of a radius?

A It is a, with the latitude and longitude being the center point of a circle, this is the radius away, the amount of meters aware that that circle should be drawn?

THE COURT: So the diameter is twice the radius?

WITNESS D'ERRICO: That is correct, yes.

THE COURT: From the point, got it. All right.

BY MR. MIKULA:

Q On row six, can you tell the Court what the display radius is on row six?

A On row six, the display radius is 23 meters.

Q Okay and so as the Court just set forth double that in meters would be the diameter, is that fair to say?

A That's correct, yes.

Q Okay and so based on what you testified previously, that the positioning could really be within, it could be as far north as 23 meters from that point of latitude and longitude, it could be as far south as 23 meters, is that fair to say?

A That's correct, yes.

Q And as far west and east?

A As Google's estimation is, it would be somewhere in that circle, that is correct.

Q Okay and you testified previously that an area let's say of 180 feet can't put a specific, you can't put a specific data point within let's say an apartment or a car, is that fair to say with the Wi-Fi data?

A Correct, using a single data point, or a single Wi-Fi data point, I cannot tell you which apartment that mobile device was originating out of. This information provides an approximate location of that device, not a specific pinpoint

location of that device.

Q Okay. The disclaimer that's on row two, do you see that?

A Yes, I do.

Q Can you read that for the Court, please?

A Yes, the map display radius fields reflects an estimated uncertainty value regarding the reported coordinate. Its value depends on a great many factors and is an approximation sufficient for its intended product use.

Q The phrase reported coordinate would that be latitude and longitude?

A Yes, it would.

Q Okay, can you tell the Court what Google considers quote, a great many factors as being?

A I would have to assume here.

THE COURT: Don't guess.

BY MR. MIKULA:

Q So you don't know?

A I don't know exactly what a great number of factors may be.

Q And you don't know how accurate or inaccurate each would be, fair to say?

A Purely from the records, that's correct.

Q Okay. Do you know if Google considers weather a factor, for instance?

A I don't know if they consider it.

Q When you see row four through eight, they all read 23 meters, is that fair to say?

A Yes.

Q Can you tell us with any scientific certainty if that figure is accurate?

A Accurate as?

Q Is it 23 meters or could it be a different amount?

A I'm sorry, I don't know what you're asking. Can you rephrase the question?

Q Well, I don't know –

THE COURT: I think the question is, you don't know from looking at rows four through eight as to those particular entries whether the 23 meters is accurate or not, is that your question?

MR. MIKULA: Yes.

WITNESS D'ERRICO: I don't know that it's one hundred percent accurate.

BY MR. MIKULA:

Q Okay, can you tell us how much variation of error there would be in the uncertainty value?

A Based on my own testing, I found these records to be quite reliability up in the seventy percentile and beyond. If it was not accurate, as in if it was a miss, if I doubled the distance of that accuracy radius, ninety percent were in that radius.

Q Does it depend on whether it's GPS, Wi-Fi or cell triangulation?

A I can tell you the GPS appeared to be more precise as in they have a much smaller radius but the accuracy of them being in that accuracy bubble, I believe are the same. I did not go out and test GPS specifically.

Q So the answer is yes, it can depend upon what source it comes from?

A The precision certainly, yes.

Q Okay.

A The precision certainly depends on the source of the data.

Q Have you spoken to Google engineers or developers about how to calculate that uncertainty value?

A No, I have not.

Q Okay, you testified previously that an average range for a Wi-Fi data point is 250 meters if it's outside?

A I wouldn't say outside. That's not the average. That's the maximum distance.

Q The maximum distance, okay.

A Correct.
Q And what's the maximum distance indoors?
A The paper said 70 meters.
Q And what paper is that?
A I'd have to refer back to my, do you mind if I refer back to one of the slides?
Q Sure.

THE COURT: Page eleven?
WITNESS D'ERRICO: I do not believe I list the source in my sources document here but I can certainly add that in. I have the information on my laptop but not in this presentation.

BY MR. MIKULA:
Q So you testified as to the maximum, do you have an idea as to what an average would be?
A You know, from an actual scientific perspective, I don't have an average. It depends on many factors such as the amount of power that's in that Wi-Fi radio.
Q What type of router it would be?
A The type, the design of the router. So each router can be a little different based on how far it can transmit.
Q How many different routers would you say are on the market today?

A I have no way to estimate that. I don't know, many.

Q How many are you familiar with?

A I know of at least six companies that manufacture routers that sell routers, they have many models from that. You know, I don't have an exact number. I mean I could say there is over a hundred, I don't have an exact number.

Q So you know of at least over a hundred, is what your testimony is?

A Well, there are likely over a hundred different routers, models and manufacturers out there. I don't have an exact listing of every router out there though.

Q Okay. With regard to, let's go to row 167 on this data exhibit. Tell me when you get there, please.

A Bottom of page four, is that correct?

Q Yes, sir.

A Yes, I'm there.

Q Okay, can you tell the Court what Google is saying the display radius in meters that is?

A 2,045.

Q Okay and if we are to assume that there are three feet in a meter, is it fair to say it's over twelve or thirteen thousand feet radius, correct? I'm sorry, that's the diameter, I was an English major.

THE COURT: Two thousand times three, it would be

around six thousand.

BY MR. MIKULA:

Q About 6500, is that fair to say, the radius?

A Approximately, that's fair.

Q Are you familiar with a router that can pick up the signal that's that far away?

A Unless it's highly modified, I don't know of a router than can do that.

Q Okay. Look at the next row if you could, 168, what does the display radius say there?

A 1,635 meters.

Q Similarly you can't testify you are familiar with a router than can pick that signal up, fair to say?

A Other than one that's highly modified, correct.

Q In your experience, what's the furthest distance that you're familiar with that a Wi-Fi router can pick up a signal?

A There was an experiment done at Black Hat in Las Vegas where they beamed a Wi-Fi signal into the desert.

Q I'm asking you in your experience.

A I don't have an exact.

MS. ULMER: Judge, objection. He was answering the question that is his experience, it's his knowledge of the setting.

THE COURT: Well, I guess the question is, is the question how far has he actually beamed a Wi-Fi signal?

MR. MIKULA: Yes, yes, sir.

WITNESS D'ERRICO: I don't have an exact figure. You know, once I leave my house, my Wi-Fi pretty much, my phone turns off Wi-Fi and goes to cellular. You know, outside of my house, I don't know, fifty meters.

BY MR. MIKULA:

Q Okay.

A Usable.

Q Right, okay, so anything over fifty meters is, are you saying somewhat suspicious?

A No, I'm saying my phone turns off at maybe approximately fifty meters from my routers being inside. That doesn't mean that the signal is not viewable or out there. It just might mean that it's not usable or it's at such a degraded capability that my phone would rather turn onto say LTE or the cellular networks. I'm not conducting traffic, you know, more than fifty meters from my house on my Wi-Fi.

Q Okay, all right.

A But I guess to finish that what I'm saying is that signal may still be visible past fifty meters. It just might not be usable.

Q Okay.

A If you're trying to connect to your Wi-Fi.

Q For a usable signal, what do you see in a standard observation presentation that you created here in this case?

A Sir, I'm sorry, I need to clarify. Are you asking what a Wi-Fi router can do or what Google has provided when marked as Wi-Fi?

Q Fair point, what a Wi-Fi router can do in terms of the distance that you generally see as a maximum?

A I don't collect information on the distances from Wi-Fi. I've collected signal strengths but I haven't collected distances from a Wi-Fi router. So I don't have any information to provide.

THE COURT: Do you mind if I asked a question?

MR. MIKULA: Yes, sir.

THE COURT: Are you saying that there is a difference between what might show up as being a signal mark on this spreadsheet and what someone may be able to use his or her phone as far as making a call is concerned?

WITNESS D'ERRICO: Yes, I am. I don't believe –

THE COURT: So someone couldn't make a call but it might show up as a hit or a printout for that particular time and date? The signal strength would be too weak to make a call but it would not necessarily for it to be too weak to show up as a data hit?

WITNESS D'ERRICO: As a Wi-Fi, correct, yes.
THE COURT: Okay.
WITNESS D'ERRICO: Yes, your Honor.

BY MR. MIKULA:
Q Looking at pages fifty and 58 if you could for a moment, let me know when you're at page fifty.
A I have page fifty.
Q Okay. And on rows 2202 and 2203, do you see the display radius that's identified?
A 2202 and 2203, correct?
Q Yes, sir.
A Yes, a display radius of four meters.
Q Okay and with regard to the source, do you see what it identifies?
A I believe it says unknown, the correct, the full value is unknown as a source.
Q Okay and what does that mean?
A That Google, when Google provided the records, they had an unknown source.
Q And look at page 58 and you see two unknowns there as well?
A Yes, I do.
Q Tell me, what rows are those on?
A 2259 and, I'm sorry, 2559 and 2560.

Q Okay and like you said you don't know how, why Google produced that information?

A No, I don't. It was obviously in their system, which is why they produced it and they marked it as unknown source.

Q Okay, if we could turn back to your presentation that you created for the day if you could. And if you could turn to page eighteen and let me know when you are there.

A I have page eighteen.

Q Okay, on this page you identified it as an observation conducted here at the Henrico County Administration Building, is that correct?

A Yes, that's correct.

Q And you show the location of the Google location services point in green, is that correct?

A That's correct.

Q All right and you show your observed location in red, is that what you're saying?

A Yes, it is.

Q Okay, did you go into the administration building and locate the Wi-Fi access point?

A No, I did not.

Q Okay. Wouldn't the location of the Wi-Fi access point give you a better observed location to compare to Google location services?

A No, it would not.

Q Why not?

A Because that is the point where I was taking my measurements from; that observed location. So what I am trying to test is what information is Google going to provide back to me when I provide it observations from that point. So regardless of where that Wi-Fi access point is, I don't need to know that. Google is making that determination when it calculates its Google estimated location.

Q But you don't know how Google identifies the access point, correct?

A I know Google's collection practice because we talked about that earlier that it crowdsources this information from billions of phones. And that was documented on its leaflet and that it was documented to the FCC in fact that Google collects Wi-Fi or collects this data using their street cars.

Q But today you can't say where the access point is in this observation, number one?

A That's correct. I don't know where the access points are.

Q Okay.

A And it was multiple access points observed if you look at the chart in the rear, page 31. You can see there is a total number of BSSIDs was 35 for that location.

Q Say that one more time?

A So the number of access points that I observed from that red point on slide eighteen.

Q Right.

A Course is documented on page 31, line one, under the column number of BSSIDs.

Q So are you saying that's the number of Wi-Fi access points where you were standing were 35?

A Where I was standing, my phone or my computer observed signals from 35 different BSSIDs or access points.

Q Okay, access points, thank you.

A And let me clarify, too, there could be multiple BSSIDs on a single access point.

Q So if you can't determine the Wi-Fi access point and you're saying Google knows that but you don't, how exactly did you decide where to place your observation point?

A I collected that observation point off my phone. I turned on my phone. I asked it for the GPS coordinates of where I was located and I plotted that on the map because that's where my computer was stationed while collecting the Wi-Fi data. So essentially that's the equivalent of me standing outside with my phone looking at my phone and Google drawing the blue dot on the map of where I was.

Q Okay, is it true that you could still get a Wi-Fi signal at other locations in the parking lot?

A I don't know, I didn't test it.

Q Okay, if you didn't locate the access point that you believe was being used by Google, how can you determine the accuracy of Google location services?

A I can determine the accuracy because I know where I was and I measure where I was from where Google estimated me to be and I can measure that distance and tell you that I was standing here at this point, the red dot on the map. And that Google was telling me that it thinks I am standing at that green point on the dot and I can measure that distance and determine the difference.

Q Okay. But isn't it true that four of the thirteen observations that you did, your observation location was outside of Google's range?

A That's correct, yes.

Q Okay and do you know why that's the case?

A I don't know why. All I know is that I sent data up to Google that was collected at those locations. Google processed it in its algorithm and did whatever it does and it sends back to me the location information of where it believes that it is.

Q Okay. Is there any reason why you chose just thirteen tests to run, or thirteen different observations let's say?

A I know it was not a, just drove around to locations

that I thought would be interesting in order to collect observations. And I tried to mix it with public buildings, you know, shopping centers, apartment complexes, townhouses, to get just a general lay in this area what this information would look like.

Q Would you agree that running more tests would give you a better point of accuracy if you did more tests than just thirteen?

A Most likely. This is a very small sample size.

Q Okay, what is the standard sample size to use in this scenario?

A Well, this was just observations. I'm not writing a scientific test or anything. This is just a sample observation of what I'm looking at. I'm not a research scientist in that area so I don't know what a standard sample set would be.

Q Okay.

MR. MIKULA: If I could have a minute, Judge.

THE COURT: Sure.

BY MR. MIKULA:

Q Can you turn to page 31 of this presentation? Are you there?

A I am, yes.

Q Okay. You were testifying previously about the, I

believe it was the RSSI maximum and minimum and the closer to zero is the more accurate it is?

A It's a stronger signal strength.

Q Okay, so how weak of a signal strength is it, what's the scale of strength for an RSSI?

A A strong RSSI would be in the negative thirty range. That's fairly strong coming off of a Wi-Fi router. And a usable signal, you know, it depends on many factors but, you know, basically once you get into negative one hundred it's unusable.

Q Okay and it's fair to say that you have ten that's listed under thirteen that is ninety or above, is that fair to say?

A For which column, the minimum, maximum or average?

Q The minimum.

A The minimum, ten, I have eleven but.

Q So eleven of the thirteen are in the ninety range, is that your testimony?

A Yes.

Q Okay and you said over a hundred is unusable?

A Pretty much, yes.

Q What are the experts in your field say about a range that's ninety to a hundred?

A It's a weak signal.

Q Okay. With regard to the Gay case that you testified to previously, did the attorneys in that case challenge the

admissibility of the Google evidence?

A No, they did not.

MR. MIKULA: I have nothing further.

THE COURT: Any redirect?

MS. ULMER: Briefly, yes, sir.

REDIRECT EXAMINATION

BY MS. ULMER:

Q In regards to the Google data, the large excel sheet in front of you, for the device tag, have you seen that exact duplicate number in any other Google location data sat that you've ever –

MR. MIKULA: Objection, asked and answered.

MS. ULMER: Actually, he was not allowed to answer that question.

MR. ACKLEY: It was stricken.

MS. ULMER: It was stricken from the record.

MR. MIKULA: I don't know if I did that but I'll stipulate to that.

THE COURT: Stipulate to what?

MR. MIKULA: I'll stipulate that that number is, I'll

stipulate that that number has not been used and has not been seen in any other, I guess, case if that was the question.

THE COURT: Well, I'd like for the witness to testify so this Court would be clear as to what the answer would be. So, did you understand the question?

WITNESS D'ERRICO: I did, your Honor.

THE COURT: And what's your answer?

WITNESS D'ERRICO: I've never seen this sequence of digits in any other Google location history data that I've reviewed.

BY MS. ULMER:

Q And then when talking about your own observations, Mr. Mikula and you were discussing that the double the accuracy radius, the Google had you within a double accuracy radius ninety percent of the time, right?

A That's correct. And the point I was trying to make is it's still in the ballpark. We're not talking about that it's at another location; that it's in Chesterfield County, that it's in Richmond City. All of these measurements were within double digit meters off and except for the last one, which was two hundred meters, I believe. It's still a relatively small number compared to, you know, the size of the universe.

Q So we're talking about miles off?

A No, we're not even miles.

MS. ULMER: Those are all the questions I have.

THE COURT: As to the points that you put into the different bubbles for lack of a better word, you took those from the entry on the assembled 59 pages, is that correct?

WITNESS D'ERRICO: That's correct. So every dot or every marking up there is, corresponds to a line in this report.

THE COURT: So it's not, there is not any, there is not a bubble for every entry?

WITNESS D'ERRICO: There is not.

THE COURT: Okay.

WITNESS D'ERRICO: I looked at certain relevant times to the investigation and plotted those out.

THE COURT: And do you know what entry numbers you have plotted on the presentation?

WITNESS D'ERRICO: I would have to go back and compare it to the time on the record to the times on the slides but there is, they do correspond.

THE COURT: My question to you is, do you know whether any of the bubbles that you used had the unknown source?

WITNESS D'ERRICO: I do know the answer and well, if I could review the slides real quick I can tell you that answer.

THE COURT: Okay.

WITNESS D'ERRICO: If I did use an unknown, it would appear in that box in the top left and that's where I detail out the number of points and what type are on that chart and the timeframes. I did not use any unknowns on these charts, your Honor.

THE COURT: Does that prompt any questions for anyone?

MS. ULMER: No, sir.

MR. MIKULA: I'd like to ask one.

THE COURT: Okay.

MR. MIKULA: Well, one quick question, Judge, if I could.

THE COURT: Okay.

RE-CROSS EXAMINATION

BY MR. MIKULA:

Q With regard to the observations you did, you used obviously your observation point as well as the range of accuracy, correct?

A That's correct.

Q Would it be fair to say that for let's say, what is the date range, for pages 39 through 45 would it be fair to say that a Google accuracy range should be used in those as well as opposed to a pinpoint drop?

A Yeah and that's a great point. By the markers on here I'm not trying to indicate that there is a pinpoint of where it is and that's why I include on the top left that block of the estimated –

THE COURT: As a range?

WITNESS D'ERRICO: As a range, right. So each point in this slide, so if I could take slide 39 as an example. On slide 39, I plotted two GPS points and 57 Wi-Fi points. Now, those two GPS points because there is only two, one of them is 13 meters and the other one is thirty meters. For the Wi-Fi points, every point in there is either somewhere between 20 and 29 meters. I could plot those on the map. It gets very sloppy and very hard to understand very quickly. So I chose to create a box instead to capture that information. And there is a scale down in the bottom right hand corner to help you determine what that range is.

THE COURT: Any additional questions?

MR. MIKULA: No, sir.

THE COURT: May the Special Agent be excused?

MS. ULMER: I'd ask him to remain for a while.

THE COURT: All right, you may step down.

WITNESS D'ERRICO: Thank you.

WITNESS STOOD ASIDE;

THE COURT: Any additional evidence for the Commonwealth?

MS. ULMER: Your Honor, the Commonwealth would like to move into evidence the presentation and for the record and to make sure we're on the same page at this time, the Commonwealth will take out slides 33 through 37 so restarting with slide 38.

THE COURT: Any objection, Mr. Mikula?

MR. MIKULA: 33 through 37, correct?

MS. ULMER: Including into that 37.

MR. MIKULA: Yes.

THE COURT: Pages 33 through 37 inclusive?

MR. MIKULA: Yes.

THE COURT: Would be taken out, any objection?

MR. MIKULA: No, sir.

THE COURT: All right, the Court will use its copy and will tear out pages 33 –

MS. ULMER: I have a copy.

THE COURT: Fair enough, all right, okay. I'm still going to do it for my copy to make sure that I don't have it.

MS. ULMER: And the Commonwealth would like to move the presentation as the Commonwealth's Exhibit number four, I believe.

MR. MIKULA: The observation presentation?

THE COURT: Yes.
MR. MIKULA: I thought that was two, so number four?
MR. ACKLEY: What was two?
THE COURT: Two would be the photographs.
MS. ULMER: The photographs, number three was the –
MR. MIKULA: The photos in Kroger.
MS. ULMER: And the jail call should be four, so this should be five. This should be five.
THE COURT: I have the number one is the first disk.
MR. MIKULA: Correct.
MS. ULMER: Yes.
THE COURT: Number two are the three pictures at Kroger.
MR. MIKULA: Correct.
MS. ULMER: Yes.
THE COURT: Number three with the Kroger ATM pictures?
MS. ULMER: Yes.
THE COURT: Number four were the jail calls and this would be Commonwealth's number five?
MR. MIKULA: Yes, sir.
MS. ULMER: Yes, Judge.

THE COURT: Number five.

NOTE: Commonwealth's Exhibit 5.

THE COURT: Anything further?

MS. ULMER: Not from the Commonwealth.

THE COURT: Any evidence for the Defendant?

MR. MIKULA: Yes, sir, Judge. Judge, I'd like to call Jake Green to the stand, please.

THE COURT: Why don't we do this? It's 12:58, we've been doing this for a little bit more than an hour. Let's take about a five minute break and everybody stretch his or her legs.

NOTE: A RECESS IS HAD; WHEREUPON THE PROCEEDINGS CONTINUE, VIS:

THE COURT: We're back on the record at 1:07 p.m. You may have a seat, sir. The Defendant is present. Mr. Mikula continues on behalf of the Defendant. Both Mr. Ackley and Ms. Ulmer are present on behalf of the Commonwealth. First witness on behalf of the Defendant?

MR. MIKULA: Mr. Jacob Green, sir.

THE COURT: Mr. Green, please.

THE DEPUTY: Would you stand for me, please?

THE COURT: Please watch your step as you step through the opening. Would you raise your right hand? Do you swear or affirm the testimony you're about to give is the truth, the whole truth and nothing but the truth?

WITNESS GREEN: Yes, sir, your Honor.

THE COURT: You may have a seat.

WITNESS GREEN: Thank you.

THE COURT: Mr. Mikula?

MR. MIKULA: Yes, sir.

WILLIAM JACOB GREEN, the witness, having previously been duly sworn, testified as follows:

DIRECT EXAMINATION

BY MR. MIKULA:

Q Could you please state your name for the record?

A Yes, sir. My name is William Jacob Green, last name is G-R-E-E-N.

Q And Mr. Green, how are you employed?

A I work with Envista Forensics in Morrisville, North Carolina.

Q What is Envista?

A Envista is a digital forensics company as well as an engineering company that assists clients across the globe. The Morrisville office is specifically a digital forensics branch of

Envista. We work with attorneys, businesses, insurance companies to interpret digital evidence and occasionally provide opinions within criminal and civil courts.

Q Okay and how long has Envista been in existence?

A Envista was previously a company called PT&C LWG. That company has been around since the nineties.

Q Okay and what are your duties there?

A I work with criminal defense attorneys as well as sometimes prosecutors in the interpretation of records, the analysis of cell phone and computer evidence, GPS evidence and then the presentation of those devices and evidence in Court.

Q Okay and how long have you been with Envista?

A A little over two and a half years.

Q Okay, going back, where did you receive your undergraduate education?

A Received a Bachelor's of Science in criminal justice from Appalachian State University in Boone, North Carolina.

Q Okay and what was that degree in?

A Criminal justice.

Q Okay and did you receive any sort of forensic experience after your undergraduate degree?

A Yes, sir. In 2006, I was hired to be a police officer with the city of Rock Hill, South Carolina, just south of Charlotte, North Carolina. I was on patrol for five years and

then moved into the criminal investigations division as a forensic investigator and assigned to our county task force to investigate crime scenes and digital evidence. In 2014, I was selected to become a part of the United States Secret Service electronic crimes task force based out of Columbia, South Carolina. The bulk of my training and experience came from 2014 on.

Q Okay and what type of crimes do you have experience with when you were with the Rock Hill Police Department?

A Everything ranging from car break-ins in the middle of the night to burglaries to, all the way up to murders.

Q Okay and you said that you were with the York County multijurisdictional forensic service unit?

A That is correct. That is the forensic task force that was assigned to our county.

Q Okay and if you could explain to the Court a little bit about your experience with electronic devices while you were with the YCMFSU?

A Yes, sir. So within our county task force, specifically and kind of happenstance, we were right next to our drug enforcement unit. They would bring in cell phones, we would utilize the police technology that was brought up by the Special Agent, Cellbrite to do the analysis of those cell phones and provide that data back to the narcotics officers. We would also

sometimes get computers and then assist with search warrants to companies like Google, Facebook, Snapchat, Twitter, to recover data that was not stored specifically on the device but stored on those servers owned by those companies.

Q Okay and in May of 2014, you left that I guess employment and went somewhere else?

A No, it was within 2014, the entire time while I was assigned to the forensics task force, my paycheck still came from the city of Rock Hill.

Q Okay.

A So I was still a police officer with Rock Hill on assignment to these locations. So I became a task force member of secret services as a special deputy U.S. Marshal and assigned to secret service for the tasks of assisting in the analysis investigation of electronic crimes.

THE COURT: You were still with the police department but you were assigned as a special secret service agent much like a special U.S. attorney would be from a state prosecutor's office?

WITNESS GREEN: Similar.

THE COURT: A designation?

WITNESS GREEN: Yes, sir.

THE COURT: Got it.

BY MR. MIKULA:

Q How many hours of experience do you have with digital forensics?

A Over six hundred hours at this point. Over 1200 hours in forensic and investigations.

Q Okay and do you have any specialized training or any specialized degrees with regard to forensic science?

A I have three certifications currently. They are in cell phone forensics through Cellbrite as a certified operator/analyst and then a computer forensics certification through a company called Black Bag Technologies.

Q Okay. And through your training and experience, have you ever investigated or been educated on Google?

A I have as a law enforcement officer and as a reviewer, typically on the Defense side, I have personally reviewed Google location services both while requesting that with a search warrant to Google and receiving a response from Google and then also through discovery practices within courts.

Q So you've dealt with Google location services in courts before?

A Yes, sir.

Q Which jurisdictions?

A Specifically, the United States Federal Court, Northern District of Ohio in Cleveland, Ohio.

Q Any other state courts?

A No, sir. I've testified as an expert in other state courts but not specifically for location history.

Q Okay. Are you affiliated with any professional memberships?

A IACIS, the International Association of Computer Investigative Specialists.

Q Okay.

MR. MIKULA: And at this time I'd ask that he be identified as an expert in digital forensics as well as location services, Judge.

MR. ACKLEY: If I could voir dire on that, please, your Honor.

THE COURT: Yes.

VOIR DIRE EXAMINATION

BY MR. ACKLEY:

Q Sir, with respect to the, you said you dealt with Google location services in a case in the Northern District of Ohio?

A Yes, sir. United States versus Sean Smith. We dealt with many location evidence pieces of which the CAST team had provided us responses from Verizon as well as Google.

Q So similar to this case?

A It was a totality of many pieces of evidence.
Q Okay, but you got a report that was similar to what has been provided to Mr. Mikula in this case?
A Similarly, yes, sir.
Q Okay and when was that case?
A That was I believe April of 2018.
Q All right and did you testify as an expert with regard to the Google location information?
A Cellular analysis with the specific location information.
Q Okay, so the cellular analysis meaning the information taken directly off of the phone itself?
A Off the phone as well as the records as provided by those companies.
Q Okay, and so you did testify as an expert and you were accepted by the court as an expert in that area?
A Yes, sir.
Q All right and but Cellbrite and Black Bag Technology primarily when you are using those you are looking at call detail records, is that fair?
A Can you repeat that?
Q When you are using Cellbrite and Black Bag's information, you are typically dealing with call detail records?
A No, sir, no. Cellbrite and Black Bag focus on the actual piece of hardware.

Q Right.

A So the cell phone and computer.

Q But I mean when you download the information, what are you reviewing in the, out of that?

A The data as it was contained within that cell phone.

Q Okay and you said sixteen hours is how much training you've had in this, I think you said –

A Over six hundred.

Q Six hundred, all right.

THE COURT: Six hundred in the digital, twelve hundred on the forensic.

MR. ACKLEY: Understood, all right. Thank you. No other questions.

THE COURT: Any objection to the designation as an expert in digital forensics and location forensics?

MR. ACKLEY: No, sir.

THE COURT: The Court will receive Mr. William Jacob Green as an expert in digital forensics and location forensics. Mr. Mikula?

MR. MIKULA: Thank you, Judge.

FURTHER DIRECT EXAMINATION

BY MR. MIKULA:

Q Let's talk a little bit about Google. How does Google

location services work?

A So Google location services is something that runs in the background of our devices. It's constantly tracking where we are going, where we've been and historically recording that within Google's methodology as they've been described through APIs, which is the actual software within our cell phones and then how that location, how that information is then taken up to the cloud and stored on Google's servers.

Q Okay, are you familiar with its intended use?

A Intended use as a consumer and as an expert is things like mapping your location, things like advertisements. They've been described already to the courts.

Q Okay, with regard to it being used as a forensic tool, are you familiar with that?

A Yes, sir, as a law enforcement officer and as an expert.

Q Okay and how long has that been used historically as a forensic tool?

A So Android, the actual operating system that is kept up with by Google has been around since about 2008. Early stages were built on a Linux platform. So Linux is an open source tool for operating systems. It's comparable to Windows or Mac. Linux is again an open source tool so the reason we have so many different variations of Android is because they are all built on that same piece of technology.

Q Okay are you familiar with the process by which Google says they collect Wi-Fi, GPS and cell data?

A To a point, yes, sir. Google has been, it's very, it's confidential and a trade secret on how and why. The vast majority of things that we do know is due to reverse engineering by people that work with the government as well as entities outside of the government.

Q Okay and has in your experience, has Google ever acknowledged ways in which to improve accuracy of their information?

A So some of the most specific ways, again going back to what's been testified, the location information is gathered and the user actually has to submit an actual affirmative response to Google during installation on the device like a cell phone. When that device, as soon as that location is approved, the cell phone will begin that transmission of data back to Google. So it's typically done that way though it can be disabled.

Q Okay and how do they speak about improving accuracy through their website and their different advertising materials that you've seen?

A So one of the most frequent ways that we see is that Google requests through the Android operating system for the user to turn on Wi-Fi to improve accuracy. If the Wi-Fi is off, the accuracy could diminish.

Q And why is that?

A Some of our most forensically valid, forensically specific locations come from things like Bluetooth connections, which are very limited in their distance and they can travel as well as Wi-Fi. GPS is very specific in the realm of location evidence and then the most, broadest would be our cellular tower services through companies like AT&T and Verizon.

Q Okay, with regard to any entities speaking on reliability, are you familiar with any studies regarding that have put forth reports on the reliability of Google's location services?

A Not necessarily the reliability of Google services. I've read scientific research papers regarding the application of Google's location services through the Google location history services but nothing specifically within the scientific methodologies for that.

Q What does Google say regarding the location services that they provide?

A Very limited. They indicate that this is a proprietary piece of technology. They do not release how and what they actually use these pieces of information for.

Q Do you know anybody outside of Google that is familiar with Google's algorithms?

A No.

Q Or the margin of error of their data?

A No.

Q Okay.

MR. MIKULA: Regarding if we could, do you mind sir placing the cellular data, or excuse me, cellular analysis survey team's presentation observation, Exhibit number five up? Thank you.

THE COURT: Would it be helpful for the witness to have what's been previous marked as Commonwealth's number five?

MR. MIKULA: I think that's a better approach, thank you, Judge.

THE COURT: All right, you're welcome.

WITNESS GREEN: Page five?

BY MR. MIKULA:

Q Yes, sir.

A Yes, sir.

Q So, I'm sorry, pages two through nine if you could look at those pages. Do you see that range of pages?

A Yes, sir, I do.

Q Okay. And you were in the courtroom previously when Mr. D'Errico testified regarding those pages?

A Yes, sir.

Q Have you seen that information before today?

A Yes, sir, I have.

Q And to your knowledge, where does that information come from?

A So the vast majority of this comes from either the privacy policies by Google as well as the terms and services of use of the Android products that they maintain.

Q Okay and is this advertising material to your knowledge?

A To my knowledge, this is the again going to back to the policies and the how and why Google or I guess more the how and, how Google is going to take this information. Not necessarily why they are taking it or what they are taking it for, so to me this isn't advertisement, this is something a business practice, not necessarily scientific research.

Q Are you familiar with any scientific research of Google's location services?

MR. ACKLEY: Objection, asked and answered.

THE COURT: I'll allow it.

WITNESS GREEN: No, sir. None that were produced by Google.

BY MR. MIKULA:

Q And if I could direct you to –

MR. MIKULA: I'm sorry, Judge, I just need to look at this a little closer. I got it today.

BY MR. MIKULA:

Q Let me go in a different direction briefly. You heard previous testimony regarding Mr. D'Errico talking about the information received by Google, did you not?

A Yes, sir.

Q Okay and that information and his qualifications he testified to having previous experience, you heard that?

A Yes, sir.

Q Within the Google location services application?

A Yes, sir.

Q Are you familiar with how CAST members are educated on this information?

A Through their testimony in courts, yes, sir.

Q Okay and where does that information come from, who educates CAST members on Google location services as well as cell phone, Wi-Fi and GPS sources?

A So much of CAST's training and experience comes form cell phone providers like Verizon, AT&T, the major carriers and that's done on an annual basis to keep those members up to speed on changes to the networks and how to interpret those reports. To our knowledge, Google has never provided training or any validation to their Google location

services reports.

Q With regard to page sixteen of that presentation, could you go to that page, please?

A Yes, sir.

Q Okay, do you have any concerns with regard to what you observed with the methodology and observation location that's identified as .2 and .2.1?

A So the biggest issues that we see here are the sample size that's used here. Thirteen, especially when we're looking at a set of data that spans over 2600 pieces of evidence that were provided by Google, thirteen is an extremely low number.

Q Okay. And if you could turn to page eighteen as well.

A Yes, sir.

Q Page eighteen, what do you see?

A So eighteen as it's been marked with the observed location, the Google location and the Google accuracy range, the Google location is a value that is assigned via a latitude and longitudinal point by Google and is actually not a fixed location. The accuracy range would indicate that the point that Google is trying to pinpoint in this area is within that accuracy range, not that specific point.

Q Okay.

A So a specific point on a map can be very misleading.

Q Okay, so with regard to the Wi-Fi access point and this kind of goes back to the previous page, page seventeen, do you, is there any sort of disclosure about the distance of the access point from the observation point that you see?

A So it's important to know, I think in the chart towards the back of the state's exhibit, the number of locations that are actually broadcasting these signals, it's important to know where that is actually coming from. You can be extremely, much more confident if you know where that is broadcasting from. And if you have a lot of network traffic being broadcast over 33 bandwidths, we need to know exactly where it's coming from in order to pinpoint that actual broadcasting antenna.

Q Okay and in terms of the and I guess is that a factor that might affect the range of the Wi-Fi router or the access point?

A Absolutely. Going back to an indoor and outdoor scenario. In my experience and my training and the research that I've seen, the theoretical distances, the numbers that were provided to the Court earlier and much safer numbers for an exterior mounted consumer antenna as we've seen in the data is more likely to be less than those described to the Court.

Q And what would you say is a more reliable figure or figures?

A So with a clear line of sight to the antenna, we can

be plus or minus fifty meters or about a hundred feet, or I apologize, that would be 150 feet.

Q And is that inside or outside?

A That would be an exterior mounted Wi-Fi antenna.

Q What about inside?

A Interior depending on the way the structure is built, concrete versus wood, glass structures more than likely less than thirty meters.

Q Okay and is that dependent upon other things as well, not just being indoors or outdoors?

A Yes, I mean there is many environmental factors, humidity, temperature, all of these things can affect wavelength and how data is transmitted over the air.

Q Okay.

THE COURT: Are you saying that you're disputing the Google accuracy radius?

WITNESS GREEN: Well, it's not necessarily the Google accuracy radius because we don't know how Google calculates that. It's the overall broadcast distance of a consumer level Wi-Fi point.

BY MR. MIKULA:

Q So with regard to, you said 150 feet or fifty meters is the most reliable or I'm sorry, can you repeat what you said

regarding what you see with regard to fifty meters and how that figure could go down or up?

A Yeah, so the numbers that were provided to the Court of over 200 meters is a very specific alteration to a Wi-Fi antenna that focuses that antenna. You don't see this in the wild. I've never experienced it in law enforcement investigations or as a defense investigator. We don't see those types of numbers in the real world. It can be done in a scientific lab for sure as it has been documented. But we don't see typical exterior mounted Wi-Fi antennas going beyond fifty meters.

Q What would you classify anything over fifty meters to be? So is it invalid or anything that you view like for instance, if I could direct your attention to Exhibit number one and I can pass this up.

A Thank you.

Q If you could go to line 167.

A Yes, sir. I'm there.

Q What is that max radius, max display radius figure?

A So Google is providing a radius of 245 meters.

Q Okay and so have you ever seen that as you classified in the wild before?

A No, sir.

Q Okay, have you ever seen a figure in the wild over fifty meters?

A It's possible. Again, depending on the type of router but fifty is really pushing what a consumer level in a residential area router would push.

Q What is a, let's say it's a consumer grade router, what do you generally, what is the figure that is reliable in your expertise?

A I think under, for an exterior mounted, about fifty meters. Interior mounted, depending on construction, thirty meters.

Q Okay, so what does that figure tell you that you see on line 167?

A This is either an anomaly or inconsistent data. It's not physically possible for two thousand meters to use Wi-Fi signal.

Q Okay, so are you saying that based on your area of expertise and your training and experience, anything over fifty meters should be considered not reliable?

A I think scientifically improbable.

Q Anything over fifty meters?

A Yes, sir.

Q What about let's say thirty to fifty meters?

A It's possible, but again it really comes down to the type of antenna pushing that signal. If it's in a residential location versus a business. Things like gas stations with exterior mounted antennas can go as far as fifty meters if not

beyond.

Q For each of these data points that you have seen in this presentation, during the life of this case, have you ever been given what the actual router style is for each of these data points?

A No, sir.

Q Okay and let's assume, well there are data points that you see in that presentation that are under thirty meters, too?

A Yes, sir.

Q Okay. Should we just accept those as being the truth?

A I think given the total nature of the data and that we don't know how and why and what Google does with this, the scientific possibilities, especially when we see huge issues of a two thousand plus meter radius, there has to be more information provided in order to be called scientifically certain.

Q Okay, did you make any calculations with how many data points are in that presentation that are over fifty meters?

A Yes, sir.

Q Okay, how many did you find?

A A little more than ten percent of the total. So if we're looking at a total of about 2600, over 260 of those are over fifty meters.

Q Okay, of the Wi-Fi data points that you observed in

that presentation, how many did you find that were over thirty meters?

A 35%, so a little more than seven hundred.

Q So approximately 35% of the data points were over thirty meters?

A Yes.

Q Okay, all right. And what concerns do you have regarding how that affects the data pool generally?

A It's we don't know. Google has provided us no documentation on how to interpret their data. We're relying on this solely based on two figures of a latitude and longitude as well as an unknown radius that we have no idea where this point lies within that radius or if it lies outside of the radius.

Q If you could, turn to page thirty of the, I'm going back to the Exhibit number five, if you could turn to page thirty of that?

A Yes, sir.

Q Tell me when you are there.

A Yes.

Q Okay. Looking at that data point and the Google, excuse me, Google location figure as well as the Google accuracy range, do you see those?

A Yes, sir, I do.

Q Can you observe where that Wi-Fi access point is coming from?

A No, sir.

Q And on observation number two, which is page nineteen, or any of these observations, have you been given what the access point is?

A No, sir, we have not.

Q How many total data points do you have in this presentation?

A I'm not sure. I believe it's thirteen, thirteen observations.

Q I'm sorry, the total number of data points in the Google data, I'm sorry.

A In the raw Google data?

Q Yes, sir.

A I believe it's 2,611, 2,608.

Q Okay. And how many of those are Wi-Fi data points?

A I do not remember off the top of my head.

Q Okay, is it the majority of those?

A Absolutely.

Q Okay. And do you have any concern with regard to the Wi-Fi access points as it relates to the cell phone data as well as the GPS data, regarding what you see with the anomalies?

A The vast majority of the anomalies do occur within our Wi-Fi ranges. So when we see going well beyond the scope

of a consumer or business of a Wi-Fi, they do occur within the Wi-Fi source, not within GPS or cellular towers.

Q The number of observation tests done was thirteen, correct?

A Yes.

Q And is that a fair number in your field to conduct this type of study?

A Not necessarily, a scientific study it would not be.

Q Okay.

MR. MIKULA: I have nothing further.

THE COURT: Any cross?

MR. ACKLEY: Yes, thank you, your Honor.

CROSS EXAMINATION

BY MR. ACKLEY:

Q A few questions. It seems like kind of your bottom line issue with utilizing Google location services in the way we are attempting to use it here is that Google has not provided the algorithms and the, if you will, exactly how they arrived at the location information that they provided to us, is that fair?

A Well, it's not necessarily the algorithms, it's the validity of this information. They provided it as an uncertain value. So we don't know how scientifically valid all of these data points are.

Q Right but in order to be able to test that validity, you have to know the algorithms, is that what you're saying?

A Yes.

Q Yes, so you know, if Google were to provide the algorithms to the scientific community and the rest of us, there would be no issue because we would be able to test it, correct?

A Correct.

Q Okay, so even though we don't know those algorithms and we don't know exactly how Google arrives at the location services data, we do know generally how it works and I think both you and Special Agent D'Errico have outlined that, right?

A Yes, sir.

Q And we do know that generally the location information that Google provides us and that it provides all of our phones when we are using our phones is generally accurate, fair?

A Yes, sir.

Q Okay, so then when I'm driving down a road and it tells me I'm on Staples Mill Road, I'm usually on Staples Mill Road or a street just adjacent to it?

A That's correct.

Q Okay. You said that the sample size of Special Agent D'Errico's observations was too small. And I think he would probably agree that thirteen is not anything to base an

entire study on. However, did you consider that also the corroboration of other data points in the, did you say 2600, how many data points, approximately 2600?

A Yes, sir.

Q So the corroboration outlined by the agent of many of those 2600 data points with other information like the jail call, like the video surveillance or the photographs that those can be added to the thirteen as part of a larger examination of the data, is that fair?

A Yes, sir.

Q Now, you said that the, you find that anything over a fifty meter range is at least suspect in your mind for accuracy?

A Yes, sir.

Q And you said that there are about ten percent were over fifty meters?

A Yes, sir.

Q Would you agree with me though that the fifty meters that they are talking about when Google provides the display radius does not necessarily mean that the point was fifty meters away from the Wi-Fi source? In other words, if the receiver, the device that we're using to try to locate attaches itself to four or five different Wi-Fi points, Google will take those four or five different and then give an approximate location, right?

A We believe it's an approximate location. We don't

know.

Q But the thing says it's an approximate location, right? It's an estimated uncertainty value regarding the reported coordinate. So that's an estimated uncertainty value, it's not necessarily an exact distance?

A It is not an exact distance, no.

Q Right, so when we are saying that anything over a fifty meter display radius means that Google is saying that the device was more than fifty meters away from the Wi-Fi point, that's not exactly accurate?

A Well, we don't know. We don't know what the display radius actually means. We can only guess.

Q So then the issue with the 2000 and I would agree with you that's probably an anomaly but the, in looking at the data, did you see how many were say over a thousand meters, I would agree that those are large distance, estimated uncertainty values, so how many were over a thousand out of the 2600?

A A few, I don't remember exactly.

Q You would agree with me that it's a very small number?

A That's correct.

Q And you would also agree with me, I think, based on your numbers that most of the display radius numbers values were less than thirty meters?

A That's correct.

Q And you are not saying that the Google location services information is inherently unreliable as a whole?

MR. MIKULA: I'm going to object. I think that's a determination by the fact finder to make.

THE COURT: I think the question calls for his opinion, which I've overruled the objection. I think you can ask him his opinion as to the reliability of it.

BY MR. ACKLEY:

Q It's not your opinion that it is generally unreliable, is that right?

A We don't know.

Q Okay. But you did agree with me that the location services that we see in a general sense is accurate?

A It's accurate to the device, we don't know exactly what it means.

Q Right. Incidentally, in reviewing your CV, it looked like you had a great deal of background in crash reconstruction as a police officer?

A Yes, sir.

Q In law enforcement. In your work in that area, did you utilize EDRs, Event Data Recorders, analyzing essentially the black box?

A Yes, sir.

Q And you're aware that, did you rely on them for information in reconstructing crash data?

A Yes, sir.

Q You found them to be reliable?

A Reliable to a point, depending on the circumstances.

Q All right and it's also true that if not all, most EDRs are proprietary and require proprietary information in order to access their content?

A Yes, but most of those manufacturers do provide guidance in interpretation of the data.

Q All right but they don't share with you the exact algorithms of how they arrived at that data, right?

A No.

THE COURT: I want to make sure the record is clear. You said right and you said no. So is it correct that they did not share?

WITNESS GREEN: They –

THE COURT: They did share or they did not?

WITNESS GREEN: They do share, they provide guidance.

THE COURT: The algorithms?

WITNESS GREEN: They do not provide the algorithms.

THE COURT: The question was, the question was, did the providers provide you with the algorithms, that was your question?

MR. ACKLEY: That's my question.

WITNESS GREEN: No.

MR. ACKLEY: I don't have any other questions, thank you.

THE COURT: Any redirect?

MR. MIKULA: No, sir.

THE COURT: May Mr. Green be excused or may he step down?

MR. MIKULA: Step down.

WITNESS STOOD ASIDE;

THE COURT: All right, any additional evidence for the Defendant? Thank you. Any additional evidence for the Defendant?

MR. MIKULA: Well, I think we could stipulate to this but I'll certainly ask the Commonwealth. I was going to call one other witness about the approximate distance from the point in which, well, actually I'll call. I was going to call regarding the distance from the apartment to where the location of the car was. Do you want me to call Mariah to say? You can object.

MS. ULMER: What exactly are you asking?

MR. ACKLEY: We don't understand.

MR. MIKULA: Just to testify regarding the distance from where the residence, from where the Defendant was living at the time to the point which where the vehicle was found.

MR. ACKLEY: I mean I can –

MR. MIKULA: I can call her and you can object.

MR. ACKLEY: Well, I mean I don't think she's going to lie. I think the issue is Mr. Mikula wants to introduce evidence that in our view is trial evidence and not germane to the motion I guess is the best way to put it.

THE COURT: I think I might need a little bit more clarification then where we are. We have the motion in limine, which moves the Court to bar the Commonwealth from presenting Google location services data. The Court has heard from the Special Agent and from Mr. Green. Any additional evidence for the Defendant?

MR. MIKULA: No, sir.

THE COURT: Any rebuttal evidence for the Commonwealth?

MS. ULMER: No, your Honor.

THE COURT: Anyone care to argue?

MS. ULMER: The Commonwealth will waive and respond.

THE COURT: Mr. Mikula?

MR. MIKULA: Thank you, Judge. Judge, what this

come down to is that the Commonwealth wants us to look at some of the data points that they can, they're saying that they can corroborate with other evidence and we should accept all the data points as a whole as being reliable. And I –

THE COURT: Let me ask you this. Would everyone agree that this concept is above the lay juror's head?

MR. MIKULA: Yes.

THE COURT: And that it would need to the extent that it is admissible with expert testimony, to the extent it is admissible would be necessary for its admissibility?

MR. ACKLEY: Yes.

MS. ULMER: The Commonwealth would agree, yes.

THE COURT: Great, okay. Mr. Mikula.

MR. MIKULA: Thank you, Judge. What I will tell the Court is, is that we have heard from two expert witnesses, both of them have testified regarding things that are certainly, require specialized knowledge and is certainly above the layperson's head as well as it takes quite a bit of education not just for the Court but also for Defense Counsel and the Commonwealth. The concerns that we have with that is it goes down to what's reliable. And so in this case, Judge, we are guided by the principles set out in Spencer regarding whether or not this information is inherently unreliable and the Court should shield the Jury from it. That's where we are.

THE COURT: Let me ask you this. What evidence

have I heard that it's inherently unreliable?

MR. MIKULA: The evidence you heard that it's inherently unreliable is the Wi-Fi data points based on Mr. Green's testimony, anything over thirty meters, which he said is something that should be taken with serious caution is over 35 is 35% of the data points are of question. There are certainly ten percent that is scientifically improbable. The question is because we don't know what Google is saying about this information, all we heard from Mr. D'Errico is what the advertising material is, is that we should accept that this data is accurate. And so that's a problem because certainly while some of it might be considered possible based upon the corroborating evidence that the Commonwealth put on today, how does that affect everything else?

THE COURT: But tell me what evidence I've heard that it's inherently unreliable?

MR. MIKULA: Row 167 of Exhibit number one.

THE COURT: Bad as to one is bad as to all? You can't believe -

MR. MIKULA: Well, we don't know. Because no one has been here to testify as to what this is.

THE COURT: Tell me how the evidence, what the evidence I've heard that the evidence as a whole is inherently unreliable. Are you telling me that row 167 because everyone believes that that may be an anomaly or an outlier within the

spectrum that that in and of itself creates the inherent unreliability of the rest of it?

MR. MIKULA: Line 167 does not in and of itself. There's more than just line 167.

THE COURT: Okay.

MR. MIKULA: There are four unknown data points. There is also up to 35 percent of the Wi-Fi data points that say that it's not, it's, we should approach it with caution and there's ten percent that says it's scientifically improbable. Not only that, Judge, you have –

THE COURT: Does it mean that there is ninety percent that makes it scientifically probable if ten percent is scientifically improbable?

MR. MIKULA: Judge, inherently, what's inherently unreliable means is in and of itself it should not be relied upon. So I guess it comes down to what the fact finder for today's purpose, which I guess would be the Court, what reliability, what calculation the Court is willing to accept. If the Court wants the ten percent makes something inherently unreliable or does the Court feel like maybe 51%. I think that's a determination or the Court to make.

But the concern here, unlike Spencer, which is a case this Court's probably well familiar with but, you know, dealt with the Southside Strangler and you had DNA PCR amplification, which was unique at that time. The

Commonwealth in that case called two witnesses, a geneticist and a serologist; both people that were trained and educated in DNA. Those two individuals testified it was something that they were familiar with that had been used in the biological field for over ten years and it was reliable. And so what's unique in this case is, is we don't know what the DNA is. Certainly, we're left to believe Jeremy D'Errico, oh, it's, well we don't know, I've never been told of any problems with it. But we should accept it. And you know, here is some, here is a PowerPoint presentation which shows that it's close to GPS. But all that data comes from Google. We don't know what the foundation is of it. We don't know what the DNA of Google is.

THE COURT: So it's your position unless the algorithms are made known to any potential expert witness, no expert can testify on Google location services?

MR. MIKULA: I think an expert has to testify that within the field it's understood what this information is and we don't know what Google information is. We don't know, even though it is certainly proprietary so I understand why they're not going to, you know, provide that information and provide that data, that formula if you will. But there is nobody else that knows about it. There is no study that's been done. They've never disclosed the rate of error.

And quite frankly, I've not heard any evidence with regard to any of the other forms of Black Box or not Black Box

but the accident crash reconstruction, even though it's proprietary, they are familiar with the error rates. They are familiar with that information. But Google, we're not. We're not familiar with any of that. And so we're left to just assume it's good information. It's turned over to the FBI and the FBI goes into Google Earth and they drop it in. And they say well, yeah, here is a range. It's not, you know, it's not this exact location but if you look at and I think raw data is a little misleading because it's raw, it gives the presumption that it's reliable. It's unadulterated.

But this is, we don't even know if that's the case. They had figures that bear serious question to whether or not this information should be assumed as a whole as being reliable. And I think the evidence has shown based upon the witnesses that while certainly there is some of this that could be considered based upon a reasonable degree of scientific certainty to be reliable, the question is, is whether the other data points, which are scientifically improbable, how does that affect the whole.

And my concern is and my argument certainly here today is that this information, there are serious questions; the data itself, not the presentation regarding the advertising but the 59 or 58 pages that all of this is, which is what we've been looking at, a lot of this information bears serious question to the reliability of this information. And that just goes to one

issue.

The other issue is, is whether this is something that should be given to a Jury to understand. And I think it should be shielded from the Jury. Why? Because for the one hand, the Jury listens to this as I'm sure most people have been watching this whole proceeding, eyes get glossed over. They're not sure what it is that they are hearing. But even more importantly than that is that we live in a digital age. People here oh, this is coming from Google and is given to the FBI and here are specific data points that are dropped onto a presentation, which even Mr. D'Errico admitted is somewhat misleading, they see that and they just think oh, well, there is no problems with it. Even if they hear from another expert witness that there is some questions as to this.

THE COURT: It's a weight issue.

MR. MIKULA: Judge, I think Spencer lays out two prongs of the analysis, whether it's unreliable, it's inherently unreliable and if the Court should shield the Jury from seeing this information or hearing this information.

THE COURT: Because of the inherentness of the unreliability?

MR. MIKULA: I think it's, I still think there are two aspects of it, but yes, certainly the second one is somewhat reliant upon the first.

THE COURT: All right, anything further?

MR. MIKULA: Judge, I just think that this evidence, the Court has to make a determination as to what inherently unreliable is. And certainly the percentages laid out and testified to by the experts go to the fact that in and of itself, it is not reliable. Thank you.

THE COURT: Thank you. Who would like to speak on behalf of the Commonwealth?

MS. ULMER: I will, your Honor.

THE COURT: Ms. Ulmer?

MS. ULMER: Your Honor, Mr. Mikula has laid out exactly what the standard is in Spencer and that is the standard inherently unreliable. This data is not inherently unreliable. Mr. Mikula's own expert Mr. Green says that he knows generally how it works and it's generally accurate when used.

In addition to Mr. Mikula's own expert, your Honor, the Commonwealth has given you many instances which show that this evidence is credible and should be given to the Jury for the Jury to determine what it would like out of this evidence.

First, Judge, this is not new technology. This is technology that has been around. You've heard from Agent D'Errico that articles were written about Wi-Fi and radio wave data since back in 2006, I believe. One article was written in 2008 that was cited by Agent D'Errico. Even Google itself

started talking about location data in their privacy policy back in 2009 and updated it in 2012 to include Wi-Fi points and cell towers in addition to the GPS. This is not a new technology.

No expert here has come out and said that there is some large study or some big paper saying that Google is a complete farce and that all of this stuff is unreliable and, you know, when you turn on your Google maps you're going to go into a lake.

Secondly, your Honor, you can use your own common sense. Google is a multibillion dollar industry. As you saw in Agent D'Errico's presentation, most of the money from Google comes from marketing. And they use Google location service and Google location systems in order to market that to their clients. They would not be in business, they would not be making the money that they make if their product, Google location data, was inherently unreliable.

THE COURT: Well, let me ask you this. Mr. Madoff, who is an investor, he had an multibillion dollar business. Was he legitimate?

MS. ULMER: He wasn't, Judge, but if the time comes when Google is found to be not legitimate then they fooled us all.

THE COURT: So we should, I believe your argument was if you are a multibillion dollar business, then you are legitimate.

MS. ULMER: No, sir, Judge. But in this instance, people rely on it. Many people have Samsung phones or Android based phones. People buy that technology. If they didn't, then everyone would own an Apple phone essentially.

THE COURT: Perhaps it's not the size of the company, it's the integrity of the company.

MS. ULMER: The integrity but I think the integrity is in this instance is outlined with the fact that this company is extremely large and that people buy into it. People choose to buy Samsung phones and not buy iPhones. People choose to use Google Maps and not Apple maps.

THE COURT: Are you saying that people are intentionally deciding to buy an Android phone because the Google location services is embedded in the phone versus buying an Apple phone that you have to download an app, is that the Commonwealth's position?

MS. ULMER: I think that people do buy Android based phones because they like the system and they like how it works and that's why they choose to do that based sometimes better than an Apple device. If the Android system itself was inherently unreliable, then who would buy the phone? No one would buy the phone.

In addition to that, your Honor, you saw in the Commonwealth's evidence the prior testing and the observations done by Agent D'Errico to show that he has

himself looked into the accuracy and the reliability of the Google data. He has also spoken to you about the Oracle study and that the data points that they collected using their methodology matched up to the points that were later provided by Google. And in addition to that, it was stipulated by the Defense that in the Gay case that the Google location services was corroborated by other evidence to show that she was at the exact points that the Google said she was at, at the same time that other evidence says that she was there.

THE COURT: Was that a stipulation?

MS. ULMER: That was stipulation and testimony.

MR. MIKULA: I don't think that I stipulated to that.

THE COURT: I'm not sure there was a stipulation to that. I believe that –

MS. ULMER: That was testimony –

THE COURT: I believe the Special Agent testified that there was separate corroboration.

MS. ULMER: Yes, sir. And so that was before your Honor. And then looking to this particular case, Judge, you can see from the data which we have presented to you that some, a lot of the data is in known locations for the Defendant; his residence, another residence belonging to Roland Anderson, not this Defendant but someone in his family. It has also been corroborated by the victim's RTT data, which has

not been said to be unreliable. It was corroborated by his text messages to and from his friend Keion. The Google location services says he was at that Tweeter Court address at approximately the same time where he tells his friend I'm at your crib, which belongs and is registered to a Keion Vaughn.

In addition to that, your Honor, you can see from the Kroger video, the GPS or the Google location data points, which are Wi-Fi data points, in addition to the GPS data points, said he was at Kroger at the exact same time that that video has Roland Anderson going into Kroger and getting, and leaving Kroger. Not only do you have the Kroger video, you have the ECO ATM receipt, which is a completely separate company which shows that Roland Anderson was at that ATM, which is ECO ATM, which is inside the Kroger, at 10:39 a.m. which is exactly the same time that the Google location points say that he is at Kroger, Judge.

There has been no evidence to say that the Google information is inherently unreliable. To the contrary, there is a lot of evidence showing that it is reliable that this is credible evidence and that should be left up to the fact finder, Judge. This is a question for the Jury. The Jury should be able to hear from Agent D'Errico about this information. And Mr. Mikula is more than welcome obviously to bring Mr. Green back and testify as to why they shouldn't listen to this information.

But it is a Jury question. The Jury does not need to be shielded from this, Judge. There has been no evidence to show that it is inherently unreliable. It goes to the weight of the evidence and that is up to the fact finder in this case. And so I'd ask that you allow this information in and to be presented before the Jury.

THE COURT: All right, thank you. The Court commends counsel on both sides for a very well presented motion in limine and defense thereof.

The Court denies the motion in limine. The Court does not find that the Google location services is inherently unreliable. The Spencer case is the seminal case for the test of admissibility of this type of information. And the Court strongly believes that the issues go to the weight of the evidence, which is a fact issue for the fact finder in this case; that is the Jury. The Court notes the exception to the Court's ruling by Mr. Mikula, counsel for the Defendant.

Anything further at this time?

MS. ULMER: No, your Honor.

MR. ACKLEY: Select a date.

MR. MIKULA: Let's choose a trial date.

THE COURT: All right and how many days will you need, we're set for three days, is that correct? It can still be tried in three days, Mr. Mikula, as far as you know?

MR. MIKULA: Yes, sir.

THE COURT: And this is set for a Jury, is that correct?

MS. ULMER: Yes, sir.

THE COURT: Okay. Mr. Anderson, did you understand the Court's ruling? I trust that you disagree with it but do you understand it, sir?

DEFENDANT ANDERSON: Yes, sir.

THE COURT: All right. How about a Monday, do you have a Tuesday, Wednesday and then I can add a Monday to it or a Thursday, Friday or excuse me, a Wednesday and we'll add a Friday to it?

THE CLERK: We have criminal like Wednesday –

THE COURT: Folks what I think we're going to need to do is to have Ms. Sanderford present with the book so that we can attempt to force something. And Ms. Sanderford is not in the courthouse this afternoon. So with everyone's permission we have to reset the setting of the case as soon as practicable. Mr. Anderson is in the custody of the Henrico Sheriff, is that correct?

MS. ULMER: Yes, sir.

MR. MIKULA: He is.

THE COURT: Okay, so his whereabouts will be approximately known or pretty close. So I was thinking perhaps next week at nine o'clock one morning or 8:45 we can have a status and set it.

MR. MIKULA: Yes, sir.

THE COURT: And then with Special Agent D'Errico's anticipated dates and Mr. Green's anticipated dates, counsel would be able to secure those. All right, what day of the week next week works for everyone?

THE CLERK: Wednesday at 8:45.

THE COURT: I'm sorry?

MS. ULMER: Wednesday the 9th at 8:45.

MR. MIKULA: I'm sorry, I can't do that date. I'm here Thursday morning or Tuesday.

MS. ULMER: I can't do Tuesdays.

THE COURT: How about the 10th, Thursday the 10th at 8:45?

MS. ULMER: We can set it for then.

THE COURT: 8:30, eight?

MR. MIKULA: Whatever time works for the Court.

THE COURT: 8:45 on January 10th for status. Anything further?

MR. ACKLEY: No, sir.

MR. MIKULA: No, sir.

THE COURT: Remanded to the custody of the Sheriff. We are off the record at 2:07 p.m. Thank you folks.

MR. MIKULA: Thank you.

MS. ULMER: Thank you, your Honor.

PROCEEDINGS CONCLUDED

STATE OF VIRGINIA,
COUNTY OF HENRICO, to-wit:

I, MEDFORD W. HOWARD, Registered Professional Reporter and Notary Public for the State of Virginia at large, do hereby certify that I was the Court Reporter who transcribed the recorded proceedings of **COMMONWEALTH OF VIRGINIA v. ROLAND ELLISWORTH ANDERSON,** heard in the Circuit Court for the County of Henrico. **I have transcribed the recording to the best of my ability to understand the proceedings herein**.

I further certify that the foregoing transcript, pages numbered 1 through 142 is a true and accurate record of the proceedings herein reported, **to the best of my ability to understand the audio recording**.

Given under my hand this 18th day of February, 2019.

/s/ Medford W. Howard
Registered Professional Reporter
Notary Public for the State of Virginia at Large
Notary Registration Number: 224566