19-8194

No: _____

ORIGINAL

In The

SUPREME COURT OF THE UNITED STATES

Jonathan Crupi,
Petitioner – Pro Se

v.

The People of the State of New York
Respondent

On Petition for a Writ of Certiorari To
New York State Court of Appeals

PETITION FOR WRIT OF CERTIORARI

Jonathan Crupi
DIN #: 15A4042
Clinton Correctional Facility
P.O. Box 2001
Dannemora, NY, 12929

QUESTIONS PRESENTED FOR REVIEW

Question 1

This court has recently decided on a case of nation-wide importance. In *Carpenter v. United States*, 138 S. Ct. 2206 (2018), this Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [Cell Site Location Information, or] CSLI." Furthermore, it was stated that "As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, religious, and sexual associations." (The later quote being the opinion of Sotomayor, J. citing *United States v. Jones*, 132 S. Ct. 945 [2012])." Thus, I present the following two-tiered question for your clarification:

Q1a. Should this Court's *Carpenter* decision on the amount of data collected from CSLI equate and extend to the amount of data collected from all digital devices?

Q1b. Does an individual maintain a legitimate expectation of privacy in the record of his digital movements through digital data collection methods?

Question 2

In recent years, there have been several cases decided by this court that could be viewed as "landmark" cases in the way that they discuss the search and seizure of electronic devices. However, many cases in the lower courts involve improper applications of particularity for searching digital devices, resulting in general, exploratory searches. Noting that some of these cases had no clear focus or limiting instructions for the search of the devices, or that the affidavits for said devices make vague connections between the crime and the devices, I ask the following:

Q2a. Have 4th Amendment rights eroded across the country due to these types of general, exploratory searches?

Q2b. Should this Court order the lower courts to examine and revise their standards for particularity and specificity with regards to the search of a digital device?

LIST OF PARTIES

[X] All parties appear in the caption of the case on the cover page.

[ ] All parties do not appear in the caption of the case on the cover page. A list of all parties to the proceeding in the Court whose judgment is the subject of this petition is as follows:

TABLE OF CONTENTS

Table of Authorities

Federal Cases

State Cases

Statutes

Other Authorities

Constitutional Provisions

PETITION FOR WRIT OF CERTIORARI

Petitioner respectfully prays that a writ of certiorari be issued to review the judgment below.

OPINIONS BELOW

The opinion of the highest State Court to review the merits appears at Appendix B and is

[X] reported at *People v. Crupi*, 34 N.Y. 3d 950 (2019).

The Opinion of the Appellate Division, Second Department appears at Appendix C and is

[X] reported at *People v. Crupi*, 172 A.D. 3d 898 (2019).

JURISDICTION

[X] The date on which the highest state court decided my case was September 19, 2019. A copy of that decision appears at Appendix B. This Court gave me until February 16, 2020 to file this application (see Appendix A)

The jurisdiction of this Court is invoked under 28 U.S.C. § 1257 (a).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The 4th Amendment of the United States Constitution provides in relevant part:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularity describing the place to be searched, and the persons or things to be seized. (United States Constitution, 4th Amendment)

The 14th Amendment of the United States Constitution provides in relevant part:

No state shall...deprive any person of life, liberty, or property, without due process of law. (see United States Constitution, 14th Amendment, Section 1)

The Supremacy Clause of Article Vi of the United States Constitution provides in relevant part:

The Constitution, and the laws of the United States shall be made in pursuance thereof...shall be the Supreme Law of the Land; and the Judges of every state shall be bound thereby, anything in the Constitution or laws of any state shall be bound thereby, anything in the Constitution or laws of any states to the contrary notwithstanding. (see United States Constitution, Article 6, Clause 2)

Criminal Procedure Law § 690.10 provides in relevant part:

Personal property is subject to seizure pursuant to a search warrant if these is reasonable cause to believe that it : (4) constitutes evidence or tends to demonstrate that an offense was committed... (CPL §690.10)

New York Penal Law §156.00 provides in relevant part:

(3) "computer data" is property and means a representation of information, knowledge, facts, concepts, or instructions which are being processed, or have been processed in a computer and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer. (see NY Penal Law §156.00- Offenses involving computers; Definition of Terms)

STATEMENT OF THE CASE

Pre-Trial and Trial Proceedings

A. A Summary of The Facts of The Case and The Trial.

Petitioner was indicted for second-degree murder based on the July 5, 2012 stabbing death of his wife, Simeonette Mapes. Both petitioner and his wife, 30 and 29-years old, respectively, were teachers at the same school in Brooklyn, New York.

The day of the murder, petitioner told police that he has left the house early in the morning, discovered his wife's body in the foyer upon returning home, and called the police. Detectives observed that entry appeared un-forced, and that although the house looked as though it had been ransacked, many valuables remained in it. Concluding that Simeonette knew her assailant, police obtained a warrant to search all computers in the couple's home and cars, and then another warrant identifying petitioner's computer specifically as a target of the search, although they had no particularized proof that petitioner had killed his wife or reason to believe that evidence of the murder was on the petitioner's computer. Defense counsel's motion to controvert these motions was denied.

The ensuing search of petitioner's internet browsing history led detectives to discover that he had been patronizing prostitutes for several years and that nine months before Simeonette's death, he has conducted online searches for throat slashing, neck snapping, suffocation, and ways to clean up blood and DNA. A number of these searches took place on Halloween, and others were intermingled with terms such as "fake movie deaths" and "unrealistic movie deaths." Although defense counsel moved to preclude this evidence on the grounds that it was prejudicial but not probative, the court deemed the evidence admissible.

At the purely circumstantial trial, the prosecutor sought to prove that Simeonette had discovered that petitioner had not obtained his Master's Degree, jeopardizing his teaching

career, and learned about his liaisons with prostitutes, and argued that for these reasons Simeonette planned to leave him, creating the motive for the killing. In support of this theory, the People introduced voluminous evidence of petitioner's relationships and communications with prostitutes, as well as the death and crime-scene related internet searches, which spanned hundreds of transcript pages and were supplemented by printouts of websites that petitioner had allegedly visited. The jury convicted petitioner of second-degree murder.

B. The Pre-Trial Litigation

I. The Search Warrants and Motion to Controvert

On July5, 2012, the People sought search warrants for, *inter alia*, "all computers, laptops, computer tablets, or cellular phones" in the home and cars petitioner and his wife, Simeonette Mapes, shared (7/5/12 Affidavit of Detective Anne Marie Murphy, Appendix E). The basis for the warrant was that:

> the number of stab wounds, the lack of any forced entry, the time of day of the stabbing, and the relationship between the victim and the 911 caller [create] reasonable cause to believe that the victim knew the assailant (*id.* At ¶ 8.) *** [C]ommunications between people known to each other are frequently transmitted electronically via email, instant messaging, social networking sites, text messages or cellular phones and therefore, there is reasonable cause to believe that evidence relating to the homicide and the identity of the victim's assailant will be found within computers or other such electronic devices capable of the above described functions that are contained within the home...of the victim (*id.* At ¶ 10).[1]

The court issued a search warrant for "computers, laptops, computer tablets, or cellular phones contained within petitioner and Simeonette's home and cars (7/5/12 Warrant, Appendix E).

A week later, police sought another search warrant, this time identifying petitioner's laptop specifically and repeating the rationale Detective Murphy had articulated in the previous

[1] Misnumbered ¶ 8.

affidavit (7/12/12 Affidavit of Detective Bryan Mason, ¶¶ 7-8).[2] The court issued a warrant authorizing a search of petitioner's computer, for "date, files, and images" (*see* 7/12/12 Warrant, Appendix E).

The defense moved to controvert both warrants, stating that there was no "probable cause to believe evidence of defendant will be found in place to be searched" (12/11/13 Motion and Affirmation of Mario Gallucci [hereinafter "Motion to Controvert"], Appendix G). Additionally, property "such as computers" "could not be specifically tied to the crime at the time the warrants were issued (*Id.* at 11).

In their opposing papers, the People claimed that the computers:

> Needed to be searched to determine what had been used, if any, before [Simeonette] was murdered, or who, if anyone, the deceased had been in contact with that could have had a reason to murder her. The computers and phones would also track time...to determine her time of death...There was certainly probable cause to believe that evidence of the fruit of the crime of murder...could be found at the location where [Simeonette] was murdered...and within the items she and [petitioner] used every day, including the home itself, their vehicles, and their computers and phones (2/22/14 Opposition of Guy R. Tardanico and Wanda DeOliveira, Appendix F).

The court summarily held that the warrants were supported by probable cause (4/16/14 Decision and Order of Hon. Leonard P. Rienzi [hereinafter :Order or Rienzi, J., Appendix D).

[2] The record is unclear as to whether the search of petitioner's computer was conducted pursuant to the first or second warrant; according to Detective Mason's affidavit, the second warrant was sought because of typographical errors in the first warrant.

II. The Motion *in Limine* to Preclude Prejudicial Evidence

The defense moved to preclude evidence from petitioner's computer, that the People sought to use at trial, demonstrating that he had searched for fatal neck injuries, asphyxiation, neck and wrist slashing, and crime-scene cleanup (*see* 6/5/15 Motion and Affirmation of Michael J. DeSantis [hereinafter "Motion *in Limine*"], Appendix H,). Describing it akin to *modus operandi* evidence, defense counsel pointed out that the searches did not correspond to the way in which Simeonette had been killed and had been conducted about nine months prior, and thus the evidence lacked probative value but was highly prejudicial (Motion *in Limine*, Appendix H).

The People also wanted to introduce testimony, online search histories, and phone records indicating that Simeonette discovered petitioner had been patronizing prostitutes, that petitioner told a prostitute to lie about her identity if anyone called asking about him, and that he obtained a disposable phone shortly after Simeonette phoned a prostitute (P. 8-13; Motion *in Limine*, Appendix H). The prosecutor believed that this evidence substantiated her theory that petitioner murdered Simeonette after she confronted him about the prostitutes, thereby constituting proof of motive.

The defense contended, *inter alia*, that this evidence was prejudicial and lacked probative value, because Simeonette's searches and calls indicated she found out about prostitutes seven months before her death, suggesting the events were unrelated, and the People failed to prove that there had been a confrontation between Simeonette and petitioner (P. 8-10; Motion *in Limine*, Appendix H).

The court found that the probative value of the death and crime-scene related internet searches outweighed any potential prejudice because this material constituted circumstantial evidence of intent or plan to kill, citing in support of it's decision *People v. James*, 93 N.Y.2d 620

(2002), *People v. D'Arton*, 289 A.D.2d 711 (3d Dept. 2011). And *People v. Murphy*, 28 A.D.3d 1096 (4th Dept. 2006).

C. The Crime Scene

Simeonette, wearing pajamas, was found lying face-down in the foyer at the bottom of the staircase to the second floor; her body, in a pool of blood, could be seen from the front doorway (Selkirk: T.T. 277; Frank Liverani [identified body]: T.T. 308-09; Saenz: T.T. 340, 379: Metsopulous: T.T. 482; Burdick: T.T. 603, 605, 607-08, 791; Cosenza: T.T 1337). There was a substantial range in the possible time of death, which could have been between 7:00 and 11:00 a.m. on July 5th, or even earlier or later (Roman: T.T. 1476, 1478-79, 1505-08). Simeonette had been stabbed three times in the neck and eleven times in the back, and had some blunt impact injuries which, along with a gate broken at the foot of the staircase, suggested that she had fallen down the stairs (Selkirk, T.T. 279; Saenz: T.T. 341, 343, 354, 399; Burdick: T.T. 607, 610-11, 780; Doctor Kristen Roman [medical examiner]: T.T. 1472, 1480-89, 1501).

The front door and locks of the home were undamaged, as were the windows, except one in an upstairs bedroom that had a mixture of DNA from three unknown individuals (Detective Robert Saenz: T.T. 391, 397, 407-08, 423, 464; Detective Michael Burdick: T.T. 604, 650; Tara Santore: T.T. 1180-81, 1187-88, 1190). The sliding glass door leading to the backyard was open about an inch (Selkirk: T.T. 280, 301: Saenz: T.T. 353, 398, 448-50, 466; Burdick: T.T. 620-21). Petitioner's palm print was on the interior, but it was not unusual for someone to have left prints in his own home (Detective Arthur Connelly [latent fingerprints]: T.T. 1052, 1054-55, 1057-59).

Most of the house was in disarray and appeared to have been ransacked, as drawers were open and items strewn about, although valuables, including jewelry and watches, bank checks, a purse and wallet, and electronics remained in various rooms (Selkirk: T.T. 279-80; Saenz: T.T. 344, 350-52, 392-93, 402-07; Burdick: T.T. 613-14, 623-26, 660-61, 701-06, 811-12, 831-37,

839-40). On a table in the foyer were a package, a set of keys, and some mail (Saenz: T.T. 391; Burdick: T.T. 609, 834-35). There was no blood on or near the dogs, whop were in crates, nor any bloody dog prints (Saenz: T.T. 351, 396; Burdick: T.T. 608-09, 612-13, 616-18, 817, 819). In the master bedoom closet was a towel with Simeonette's blood on it (Saenz: T.T. 427; Rachel McClonskey [criminalist]: T.T. 1154-56), and a jewelry box that had a mixture of DNA from three individuals, none of whom were petitioner, Simeonette, or Katie Smith (*alias*) (Santore: T.T. 1179-80, 1186-87).[3]

Petitioner and Simeonette's laptop bags, which held their computers were found in a hall closet located immediately off the foyer; the closet was so close to Simeonette's body that one would either have to stand over her or to her side to open the closet door (Saenz: T.T. 363, 370, 408, 434-36; police Officer Michael Fantry: T.T. 4788-79; Burdick: T.T. 612, 768, 778, 785-86; Cosenza: T.T. 1233-34).

On July 13th, petitioner did a "walkthrough" in the presence of detectives to determine what might have been taken from the home (Burdick: T.T. 689, 862). After about nine months, having looked in the bedrooms for only seconds, petitioner said that he was finished, and his attorney sent a follow-up email listing items that petitioner thought might have been missing (Burdick: T.T. 690-96, 860-62; Peo. Ex. 163).

D. The Evidence from Petitioner's Computer

The morning of October 9, 2011, petitioner had searched Google for "neck snap" and then clicked on a discussion thread entitled "[o]n a human, does neck snap equal instant death"

[3] DNA that probably belonged to petitioner and Simeonette was found in various areas of the home (Saenz: T.T. 414-19, 449; Santore: T.T. 1181-83).

(Detective Jorge Ortiz: T.T. 910; Cosenza: T.T. 1240-42, 1357-58; peo. Exs. 200, 216). The question continued:

> In action movies, whenever the hero and his posse are trying to infiltrate the bad guy's lair, they will often try to get rid of various guards and henchmen by performing silent kills....The clichéd way to do this is to sneak up on the bad guy and snap his neck. It is shown that the neck snap is instantly incapacitating. But is the neck snap lethal in itself or does it result in below-the-neck paralysis that eventually leads to suffocation...? (Cosenza: T.T. 1242-43, 1357-60; Peo. Ex. 216).

A number of subsequent responses were about the consequences of a broken neck in real life, and the prosecutor elicited one, on the fourth page of answers, suggested using a knife to kill someone instead, as "if you want to kill someone quickly...the knife is much better instrument than any hand-to-hand technique" (Cosenza: T.T. 1243-44; Peo. Ex. 216). At the same time, as defense counsel brought out during cross-examination, many responses showed that users were merely curious about scenes they had seen on television (Cosenza: T.T. 1360-62; Peo. Ex. 216). The same day, about two and a half hours later, petitioner searched for "laugh out loud comedy strips," "fake movie deaths," "unrealistic movie deaths," "unreal movie deaths," and 'Easter eggs transformers dark of the moon" (Ortiz: T.T. 971, 975-77; Cosenza: T.T. 1343-47, 1354-56, 1358-59: Peo. Ex. 200).

The following afternoon, around 1:00 p.m., searches for "sleep" "suffocation," "asphyxiation," "pillow suffocation," and "pillow suffocation and death" were conducted, and related webpages visited (Ortiz: T.T. 911-12; Cosenza: T.T. 1244-47, 1363; Peo. Exs. 200, 217-22). Pages of questions and answers pertaining to these searches were introduced into evidence, many of which the prosecutor had Cosenza read aloud (Cosenza: T.T. 1247-52; Peo Exs. 217-22). One response, in a forum discussion entitled, "is death by pillow suffocation only a myth?" that the prosecutor specifically elicited from Cosenza read:

> If you hold a pillow over someone's face it would indeed obstruct their air flow to the point where they wouldn't get enough oxygen and pass out. If they continue to have obstruction, then they will die. This takes some time though. It is never as fast as in the movies. The pressure doesn't matter so much (Cosenza: T.T. 1248; Peo. 218).

The prosecutor drew Cosenza'a attention to a webpage about suffocation, asking him to read from a subsection entitled "homicidal smothering":

> Homicide is possible where the victim is incapacitated from drink or drugs, a very weak child or old person in ill health and when the victim is stunned by a blow. Usually the mouth and nose are closed by a hand or cloth or the face may be pressed into a pillow (Cosenza: T.T. 1251; Peo. Ex. 21).

Defense counsel elicited that some responses referred to movies, and that the only one the prosecutor had Cosenza read aloud was the paragraph about homicidal smothering, while there were others about accidental and environmental smothering (Cosenza: T.T. 1369-70).

At 1:00 p.m. on October 11, petitioner had searched for, among other terms: "throat slasher," "throat slash," and "how to slash throat," and visited webpages related to these queries (Ortiz: T.T. 914: Cosenza: T.T. 1254-59, 1266, 1372, 1407; Peo. Exs. 200, 222-25).

Petitioner had conducted a number of Halloween-themed searches the morning of October 31 (Ortiz: T.T. 916, 996-99; Cosenza: T.T. 1260-61, 1357; Peo. Ex. 200). Then, there were several searches for "bleach," "blood stains," "crime scene," and 'DNA," and petitioner had accessed webpages- including one called "homicidesquad.com/crimesceneinvestigation" and another with the title question "what destroys DNA"- explaining the most effective methods and products for removing blood

stains, which include hydrogen and sodium peroxide (Ortiz: T.T. 916-19; Cosenza: T.T. 1261-63, 1266-73, 1338, 1379-80, 1383, 1385-88, 1405, 1408-09; Peo. Exs. 229, 227-31).

A webpage entitled "The Reality of Crime Scene Investigation part II" was also accessed (Ortiz: T.T. 918-19; Cosenza: T.T. 1268-69, 1271-72, 1274; Peo. Ex. 232). The prosecutor had Cosenza read aloud a paragraph at the end of the second page:

> Even criminals are not immune to the CSI effect...criminals can benefit by watching CSI shows to learn how to cover their tracks more effectively...Criminals learn to clean crime scenes with bleach to destroy DNA and wear gloves to avoid leaving fingerprints (Cosenza: T.T. 1274; Peo. Ex. 232).

Apart from those discussed above, there were no death- related queries among the 60,000 in the search history (Ortiz, T.T. 908-09, 911, 913, 915-18, 969-70, 979-80, 993-95, 1002-04; Cosenza: T.T. 1238, 1253-54, 1339, 1342-48, 1356, 1367-68, 1373, 1375; Peo. Ex. 200). Petitioner searched for "what are some foods you can eat to produce more sperm" on November 8 and for Wicked tickets on December 14, 2011 (Ortiz: T.T. 1005-06).

E. The Summations

Defense counsel argued the People failed to prove that there had been a confrontation between petitioner and Simeonette, that there was evidence they were a happy couple, that none of the crime scene evidence pointed to petitioner as the killer, and that several witnesses altered their trial testimony from earlier statements in order to guarantee petitioner's conviction (T.T. 1560-65, 1570-77, 1580-81, 1588-91, 1595-96). The internet searches were not inculpatory, because people conduct all sorts of Google

searches, and many of petitioner's death-related queries were made in the context of television and film (T.T. 1600).

In her summation, the prosecutor contended that the evidence showed escalating conflict related to the prostitutes and Master's Degree, allowing jurors to surmise that there had been a confrontation the morning of July 5 (T.T. 1609-25, 1633, 1640-41). She cited the following as evidence of petitioner's guilt: his browsing history, Ross' testimony that the couple did not need anything from the school to teach summer classes, the lack of forced entry, petitioner's palm print on the door, the valuables remaining in the house, the neighbors not seeing anyone, the absence of bloody dog prints or blood on the dogs, and petitioner's short walk-through in July (T.T. 1631-32, 1636-37, 1639, 1643-46, 1648, 1650-52, 1654-59). That the throwaway phone and laptop bags were in the hall closet, immediately behind Simeonette's body, showed that petitioner either stepped over or around her to place these items in the closet, the prosecutor contended, belying his claim that he came upon her body and entered in a state of shock (T.T. 1633, 1653-54, 1659-61). Similarly, witnesses testified about his lack of emotion immediately following the incident, again pointing to his guilt (T.T. 1629-31).

F. The Motion to Dismiss, Charge, and Verdict

Defense counsel moved to dismiss the second-degree murder charge, arguing that the People had failed to prove anything beyond marital discord (T.T. 1525-26, 1532-33). After the People opposed, the court stated that it would reserve decision on the motion, although it never issued a decision (T.T. 1526-27). All parties agreed to dismiss the fourth-degree weapon possession charge (T.T. 1526-33).

The court instructed the jury that the evidence prostitution could be used only for the limited purpose of demonstrating proof of marital discord (T.T. 1679-80). The jury convicted petitioner of second-degree murder (T.T. 1702-06).

G. The Direct Appeal and Leave Application to the Court of Appeals.

On or about April 3, 2018, petitioner's counsel filed her brief with the Court of Appeals. In it, she raised 4 grounds. Those being:

Point I:	The people failed to prove petitioner's guilt beyond a reasonable doubt and the verdict was against the weight of the evidence, because they established nothing concrete beyond petitioner being an unfaithful and deceitful husband, and that the entry was unforced and no property stolen.
Point II:	The court erred when it allowed the people to introduce a massive amount of non-probative, prejudicial evidence that petitioner had (A) conducted internet searches for "neck snap," "throat slash," "suffocation," and others pertaining to cleaning up blood and DNA, nine months before Simeonette was stabbed to death and; (B) patronized prostitutes during and after their marriage.
Point III:	The court erred when it refused to grant the defense motion to controvert two warrants allowing police to search petitioner's computer, because they (1) failed to assert reasonable cause to believe that evidence of the murder would be found on the computer and (2) were overbroad.
Point IV:	The court abused it's discretion and deprived petitioner of a fair trial by prohibiting defense counsel from cross-examining a detective who played a crucial role investigating this case about allegations of police brutality underlying a federal lawsuit, and by quashing defense counsel's subpoena for CCB records related to the lawsuit.

On May 8th, 2019, the Appellate Division, Second Department, denied petitioner's appeal, holding, amongst other things that (a), each of the challenged warrants was supported by a an adequate police affidavit, (b), the warrants were not overbroad, (c), the searches of devices was not improper, (d), the court exercised its discretion in prohibiting the cross-examination of a police witness, and (e), the

introduction of evidence was relevant. Petitioner's counsel filed an Application for Leave on July 1st, 2019 and was subsequently denied on September 19th, 2019.

II. Reasons Why This Court Should Grant Certiorari

This case represents the perfect platform for this Court to inquire into several areas of national importance ahead of the technological wave that will continue to be implemented in our daily routines as citizens of the future.

1. This Court's *Carpenter* holdings should equate and apply to all digital devices.

Cell phones have become such an important tool in our lives over the last two decades, that is becoming increasingly harder to imagine a life where information was *not* available at our fingertips. Now we can merely speak our demands, and our smart-phones comply, neatly interpreting exactly what we are looking for and reporting the data back to us via the pleasant voice of the phone's artificial intelligence. This Court cites a study that found that "nearly three-quarters of smart phone users report to being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. See Harris Interactive, 2013 Mobile Consumer Habits Study [June 2013]" (Riley v. California, 573 U.S. 373 (2014). When discussing "The Internet of Things", Sara Shahmiri cites that "given that 5.5 million new devices get connected daily, studies predict that over 20.8 billion devices will be in use by 2020." (see Sara Shahmiri, *Wearing Your Data on Your Sleeve: Wearables, the FTC, and The Privacy Implications of This New Technology*, 18 Tex. Rev. Ent. & Sports L. 25 [2016]).

Additionally, as these billions of devices become more intricate parts of daily life, more and more data will be stored on them. Peter A. Crusco expands on this idea,

putting it into a legal scope, saying "...the sheer breadth of potential data, and therefore potential evidence of criminality, that may exist on a target's digital platform, such as his or her mobile phone, tablet ,or computer, to name a few, many times causes the defense to test the particularity of the search warrant." (see Peter A. Crusco, *The Old Particularity in New Digital Raids,* New York Law Journal, October 24, 2017.)

As Crusco implies, these devices contain mountains of information. So much so, that entire lives can be re-constructed by a thorough search of the information stored on them. But what is the constitutionality of searching these devices? When is the search of these devices too broad?

The case law regarding searches of "smart" cellular phones, tablets, and computers is rapidly evolving, due to the speed of which such devices have become essential to modern life, as well as the amount of personal information they tend to hold. *See, e.g., Riley V. California*, 134 S.Ct. 2473 (2014); *Unites States v. Galpin*, 720 F.3d 436, 446 (2dCir. 2013). The general trend is toward a recognition that particularized probable cause is of the utmost importance when it comes to searches of computers and smart phones, as these devices are "capable of storing immense amounts of information and often contain a great deal of private information" so that searches of them "often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers." *United States v. Payton*, 573 F.3d 859, 861-62 (9th Cir. 2009); *see Galpin*,720 F3d at 446 ("The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous...and compounded by the nature of digital storage"); *People v. Covlin*, 58 Misc. 3d 996 (Sup. Ct. N.Y. Co. 2018) ("[t]his court's own anecdotal experience indicates that the kind of non-particularized warrants for digital data at issue here are all too common in New York").

This Court has also previously ruled on these issues in *Carpenter v. U.S.*, 138 S. Ct. 2206 (2018). "Mapping a cell phones location over 127 days provides an all-encompassing record of the holders whereabouts." *Id.* This brings up privacy concerns, where this Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through Cell Site Location Information (CSLI)." *Id.* Now, it is widely accepted that the current generations of smart phones are an all encompassing tool for the modern citizen, with features ranging from simple talk and text, to web access, gaming, photo editing and sharing, and several other practical applications. The question we are concerned with here is this: How are these phones and digital devices different from each other?

Truth be told, they aren't. Sure, some functionality may be *essentially* different amongst them, but many devices serve the same basic purposes: talk, text, web access, gaming, photo sharing...the similarities are astonishingly similar. Therefore I suggest that this Court's holdings from *Carpenter* be applied to all "digital devices," which would include phones, tablets, laptops, computers, and wearables. Any digital device that shares the same basic functionally of a smart phone should be afforded the same protections that our Constitution upholds for cell phones.

2. The average citizen has a legitimate expectation of privacy in the record of their digital movements, especially when a search warrant offers unrestricted access to an individual's digital life.

Given this shift in the distinction of a digital device, the privacy issues that arise are phenomenal. In this era of surveillance as we now live in, Americans expect a reasonable amount of privacy in their daily lives. A reasonable person would expect this

privacy to extend to their cell phones as well, and as we have been discussing, all of their digital devices. As this Court states in *Carpenter,* "the time stamped data [found on a digital device] provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.' (opinion of Sotomayor, J. citing *United States v. Jones* 132 S. Ct. 945)"

Having unrestricted access to all of this data is the *definition* of invasiveness, and this questions our 4th Amendment rights as they are applied to the searches of our digital devices, specifically, our right to privacy. This "intimate data" that Sotomayor speaks of holds a far more distinctive snapshot of someone's life than, say, a diary would in the pre-digital age. A diary would only inform the reader of whatever information was input into the diary. A digital device, however, stores and saves all types of data, ranging from location, time and date stamps, a web search, an intimate message between consenting adults...who is to say that all of this information is up for grabs when the police search the device with an overbroad, unrestricted search warrant?

If we now switch our focus and examine The United States Court of Appeals decision in *United States v. Galpin* , 720 F. 3d. 436 (2013), we begin to see the privacy issues that arise from the search of digital devices. The court stated :

> As numerous courts and commentators have observed, advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain...The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous. This threat is compounded by the nature of digital storage. *Id*

Further, we see the court discuss the necessity of particularity in these situations:

> Once the government has obtained authorization to search the hard drive, the government may claim that the contents of every file it chose to open were in plain view and, therefore, admissible even if they implicate the defendant of a crime not contemplated by the warrant. There is, thus, "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." (*United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 [9th Cir.2010]) This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches." *Id.*

The ideas expressed in these two passages are complex, and touch on a variety of topics, such as particularity as well as the plain view doctrine. We will discuss the implication of these ideas later on, but here it is important for us to pause and reflect on how searches of these kinds do, in fact, violate the 4th Amendment. Crusco helps us to do this efficiently. He says:

> In Galpin . . .both courts acknowledged that searches of computers often involve a degree of intrusiveness much greater in quantity and kind from searches of other containers, but Galpin involved a search warrant authorizing a broad search of defendant's computers "for evidence of violations of NYS Penal Law and or Federal Statutes," which did not provide the officers executing the warrant with any guidance as to the type of evidence sought, thus violating the particularity clause of the Fourth Amendment. (see Crusco, The Old Particularity in New Digital Raids, p. 3)

Crusco's analysis of the Galpin case gives us food for thought. Think about the amount of data stored in the devices in question. Broad warrants, like the ones in question in the Galpin case, offer the officer executing the search warrant unrestricted access to an individual's digital life, and in the technological day and age that we live in now, this is an invasion of privacy in every sense of the matter.

3. 4th Amendment rights have constantly come into question in the last few years when particularity requirements have been applied to the searches of digital devices.

We have already discussed the implications of these general, exploratory searches, but let us now look forward to how the courts have ruled on the ideas of the plain view doctrine and particularity. In *Coolidge v. New Hampshire,* 91 S. Ct. 2022, this court ruled that "...the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges." This is a prime example of what happened in my case. The detective searched through 60,000 lines of data until he found something questionable in the form of Google searches from nearly nine months before my wife was murdered . The detective testified that his examination of all this data took days upon days, and that he conducted his research both at work and at home. (Cosenza: T.T. 1339-48, 1354-56, 1367-68, 1373-77) Where was the particularity here? Why was he allowed to access data from so far back in time?

In *United States v. Carey,* 172 F.3d 1268, the court quotes the above statement from Coolidge, but also goes on to question the scope of warrants:

> The warrant obtained for the specific purpose of searching defendant's computers permitted only a search of the computer files for 'names, telephone numbers, ledgers...' The scope of the search was thus circumscribed to evidence pertaining to drug trafficking. The government's argument [that] the files were in plain view is unavailing because it is the contents of the files and not the files themselves which were seized. *Id.*

To compare this to my case, the Google searches in question fell into the lap of the detective searching through 60,000 lines of data, an enormous amount by any standard. Such an invasive search can not be viewed as upholding the plain view doctrine. Months

and months of data was gone through with a fine tooth comb. The intensity of the search is not what I am questioning though. When we remember that the searches were done nine months before the crime occurred, again, it only makes logical sense to conclude that the searches were overbroad, generally exploratory, and unconstitutional.

Even the language used in the warrants themselves is broad and general. If we examine New York Penal Law §156.00, we see the following:

> (3) "computer data" is property and means a representation of information, knowledge, facts, concepts, or instructions which are being processed, or have been processed in a computer and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer. (see NY Penal Law §156.00- Offenses involving computers; Definition of Terms)

To the average person, this definition would translate to "any and all information stored on the device." The use of this phrase, "computer data, files, and images," (See Appendix E) in the warrant itself is an error, along with the State's definition of such. If we were to examine the State's weak affidavit application for the warrants, we see that the reasons for the search of the computers was because "communication between people known to each other are frequently transmitted electronically via email, instant messaging, social media sites...", and that "the victim [may have known] the assailant." (see Appendix E- emphasis added) This general, exploratory search for any evidence of "murder" was completely overbroad, especially when we remember when they had originally intended to examine e-mail addresses and social media accounts. Again, these reasons may lend probable cause, but they led to an overbroad search of the computers.

The United States District Court of West Virginia's decision in a recent case may shed some more light on the issues at hand. They held that, when examining the concealment of certain documents, that:

> This consideration does not negate the initial particularity requirement. This only allows for an expansive and broader search warrant when a known file or document could

> masquerade as another. This warrant did not even mention what document, file, or information for which law enforcement was searching. As such, a broadly written warrant would not be appropriate under these circumstances. (*United States v. Cobb* 2018 WL 6273480)

The court goes on to further state that "The fact that certain warrants impliedly allow a cursory review of the documents does not negate the particularity requirement." *Id.* And that "This is not a cursory review of the documents and files to determine whether they fall within the scope of a warrant; this was rummaging to see what was on the computer." *Id.* This is exactly what happened when the detective looked though months and months of data, 60,000 lines to be exact. It was a rummaging, looking for anything that could be used against me until as stated in *Coolidge* "something incriminating at last [emerged]" (*Coolidge*- emphasis added).

4. There is a need to harmonize with the lower courts to protect the rights that the 4th Amendment ensures.

Looking back at Crusco, he reminds us of the importance of particularity in cases like this. "Particularity has as its goal that the search will be carefully tailored to its purposes and will not take on the character of a wide-ranging general exploratory search or 'rummaging' that the Fourth Amendment prohibits." (Crusco, p.1) Furthermore, he describes the implications of particularity through the lens of digital searches:

> Particularity requires specificity, which not only protects one's right to privacy but leaves little discretion to the executing officers...Particularity in the description of what is to be seized [and searched] under the warrant serves as a limitation in a digital search, for instance, for what files on an electronic device may reasonable be searched. Particularity deficits undermine the presumption of legality that accompanies the issuance of a search warrant. Challenges on these grounds have only increased when computer searches are involved because of the nature of a digital search. (Crusco, p. 3- emphasis added)

All of the ideas Crusco expresses can be applied to the search warrants in question here. They were overbroad, had no limitation, and left plenty of discretion to the executing officer, which was demonstrated by the search of information from nine months prior to the crime.

This raises another issue: Staleness. Admittedly, the issue of staleness usually takes issue with the passage of time between the information and the probable cause for the warrant itself. However, when we examine the concept of staleness in a different light, we see a different issue at hand. Recently, *United States v. Crawford*, 2019 WL 3207854 passed ruling in the issue. The court stated:

> Where the facts occurred too far in the past to give rise to probable cause that evidence of a crime will be found in the location sought to be searched, the facts are said to be stale...When exactly facts become stale and probable cause expires "is determined by the circumstances of each case...and depends on the inherent nature of the crime." Staleness cannot be measured "solely by counting days on a calendar." "The passage of time becomes less significant when the crime at issue is ongoing or continuous..." (*Id,* citations omitted)

It is important for us to remember the circumstances of my case. The searches occurred nine months before the crime. Also, the searches only occurred one time, and were only viewed momentarily, for extremely short lengths of time. (Cosenza: T.T. 1339-48, 1354-56, 1367-68, 1373-77)

To relate to this, *People v. Hulland*, 110 Cal. App. 4th 1646 (2003) refers us to the following: "If circumstances would justify a person of ordinary prudence to conclude that an activity had continued to the present time, then the passage of time will not render the information stale.' (citing *People v. Mikesel,* 46 Cal. App. 4th 1711, 1718 [1996]). I challenge that the contrary is true in my situation. The activity in question never continued, and was a solitary event when we compare it to the 60,000 lines of

information at hand. Therefore, the passage of time between the information found (the fruits of the search) and the crime itself makes the evidence "stale".

So not only were the warrants executed unconstitutionally, but the information that was "incriminating" occurred at such a distant time from the crime itself that the information found is inadequate. There was no "continued activity", as accentuated above. Furthermore, if the People sought to prove that intent was shown by these searches, and that the wheels were in motion for so long a time, does that not mean that there was a pre-meditated element to the crime? I was not charged thusly, only receiving a charge for second-degree murder along with a fourth degree weapons charge that was subsequently dropped because no murder weapon was ever produced.

To close, I direct you attention to *United States v. Williams*, 592 F.3d, 511(2010):

> ...at its core, the 4th Amendment protects against general warrants that authorize "exploratory rummaging in a person's belongings...by requiring a particular description of things to be seized." (*Andresen v. Maryland*, 427 U.S. 463, 480. [1976])" *Id.*
>
> ...when a search requires review of a large collection of items...documents not covered by the warrant [are improperly seized;] the government should promptly return the documents or the trial judge should suppress them. (*see Andresen*, 427 at 482) *Id.*
>
> Whether seized evidence falls within the scope of a warrant's authorization must be accessed solely in light of the relation between the evidence and the terms of the warrants authorization. *Id.*

These quotes sum up the questions at hand here. 4th Amendment right have eroded across the country. Many of the cases we have examined here would *never* have been brought forth if the correct action was taken to begin with. This Court needs to set the record straight with the lower courts to ensure that this Courts rulings are upheld, being the "Supreme Law of the Land." (see United States Constitution, Article 6, Clause 2)

Conclusion

While this case is important to the petitioner, in that I, Jonathan Crupi, will have to serve a life sentence for a crime I did not commit, there are matters involved which are more important. First: the protection of the rights of other citizens is involved, and second: the obedience of the States to the mandates of this Court is involved. If the questions presented by this case have not already been answered, then they are questions that this Court should answer, because they are recurring questions of critical importance in the administration of criminal law.

Based on the law and facts articulated above, I am requesting that this Court issue an order granting certiorari on any and all questions and arguments raised above, and for any other and further relief as to this Court may deem just and proper.