Case No. 4-422

IN THE

Supreme Court of the United States

October Term 2017

UNITED STATES OF AMERICA,

Petitioner,

v.

AMANDA KOEHLER,

Respondent.

On Writ of Certiorari

to the United States Court of Appeals

for the Thirteenth Circuit

BRIEF FOR RESPONDENT

AMANDA KOEHLER

Team 14

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Secondary Sources

STATEMENT OF ISSUES

I. This Court Holds That Electronic Data Storage Devices Require Greater Protections Than Other Types of Property Due To The Vast And Extremely Private Nature Of the Files, And Circuit Courts Hold Non-Routine Searches Of Electronic Data Storage Devices Require Reasonable Suspicion, And Ms. Koehler's Entire Private World, Including Hundreds If Not Thousands Of Personal Files, Were Ransacked Without Any Limitation On The Duration Or Scope Of The Intrusive Search. Did The Thirteenth Circuit Properly Reverse the District Court's Denial Of The Motion To Suppress Finding Agent Ludwig Lacked The Requisite Reasonable Suspicion To Conduct A Non-Routine Search?

II. Under The Fourth Amendment, A Person Has The Right To Be Protected From Unreasonable Government Searches, Especially In Her Own Home. Here, In Order To Undergo A Warrantless Investigation Of Ms. Koehler's Home And Adjacent Property, The Government Hovered A Drone Equipped With A High Powered Camera Over Her Property For Fifteen Minutes, And Scanned The Buildings With A Radar Device That Can Measure The Breath And Movements Of Inhabitants. Did The Government Violate Ms. Koehler's Fourth Amendment Protections?

STATEMENT OF FACTS

Eagle City border station is on a major crossing point between the U.S. and Mexico, and the U.S. Border Patrol prioritized securing the Eagle City border station by assigning more Border Patrol Agents to Eagle City than any other border station in the U.S. R. at 2.

On August 17, 2016, U.S. Border Patrol Agent Christopher Dwyer and his partner, Agent Ashley Ludgate, were on patrol at the Eagle City border station around 3:00 A.M. when they stopped a car driven by Scott Wyatt. R. at 2. When asked why he was crossing the border into the U.S., Mr. Wyatt appeared disconcerted and unhelpful. R. at 2. When Agent Ludgate asked Mr. Wyatt if he was transporting $10,000 or more in U.S. currency, Mr. Wyatt said he was not, and then Agent Ludgate informed Mr. Wyatt of their right to search his vehicle and that this was a routine search done on every vehicle. R. at 2. Agent Dwyer asked Mr. Wyatt to step out of the car and open his trunk, and when Mr. Wyatt opened the trunk, he discovered $10,000 in $20 bills and a laptop with the initials "AK" inscribed on it. R. at 2. Suspicious of the contents, Agent Ludgate asked Mr. Wyatt if the laptop was his, and Mr. Wyatt stated that he shared the laptop with his fiancé, Amanda Koehler. R. at 2.

When the agents ran Ms. Koehler's name in its criminal intelligence and border watch database, the search revealed that Ms. Koehler is a felon with multiple convictions for crimes of violence, and Ms. Koehler was also named as a person of interest in the recent kidnappings of John, Ralph, and Lisa Ford. R. at 2. The Ford children were kidnapped on their way to school and held for a ransom of $100,000 each, and recently, the kidnappers agreed to give proof of life (in the form of a phone call with one of the children) in exchange for $10,000 in $20 bills, due at noon the following day, August 18. R. at 2.

The FBI and Eagle City Police Department (ECPD) have been working together, as they believed the Ford children were transported across state lines and held somewhere in Eagle City. Aware of the ongoing investigation, Agent Ludgate opened the laptop and began looking through the desktop of the laptop. R. at 2.

When Agent Ludgate opened the laptop, she found several documents on the desktop, and some of these documents contained Timothy H. Ford's personal information, such as Mr. Ford's address, a list of Mr. Ford's upcoming meetings and appearances, and the names of his staff members. R. at 3. Agent Ludgate continued searching through the documents and found a lease agreement with the name "Laura Pope" and an address that did not match Mr. Ford's, so Agent Ludgate informed Agent Dwyer of what she found and placed Mr. Wyatt under arrest for failure to declare in excess of $10,000, a violation of 31 U.S.C. § 5136. *Id.*

Agent Ludgate joined Detective Raymond Perkins, the lead detective on the kidnapping case, and soon discovered the address was for Macklin Manor. *Id.* This building was a large estate on the top of Mount Partridge, which was on the outskirts of Eagle City. *Id.* The Manor is in an area usually covered in clouds and fog all year. *Id.* Planes almost never fly over the area because of "extremely limited visibility." *Id.* Around 4:30 A.M., two police officers were sent to surveil the manor. *Id.* One officer walked around the property, and the other, ECPD's technology expert, flew a PNR-1 drone over the home. *Id.*

The PNR-1 drone costs $4000, is capable of going 30mph, and has a battery life of 35 minutes. R. at 38. While available for limited public purchase, the PNR-1 was "specifically designed for law enforcement," who often favor the device for its discreet design, high definition DLSR camera, and video-taking capabilities. R. at 46. As to storage, it can hold 15 minutes of video and 30 still photographs. R. at 3. It is pre-programmed to not exceed an altitude of 1640

feet, but has had a glitch that allows it to fly up to 2000 feet. R. at 4. According the ECPD, it exceeds its legal limits around 60% of the time. R. at 41.

After being launched, the PNR-1 flew around 7 minutes to get to the manner, hovered over the home and its surrounding property for 15 minutes, and flew the 7 minutes back. R. at 4. Because of the typical low visibility, there were no other aircraft seen or heard. R. at 38. The drone recorded 22 photos and 3 minutes of video of Macklin Manor. R. at 4. These showed the estate consisted of a large main house, an open pool, patio, and pool house. *Id.* There was also an image of a young female person walking from the main house to the pool house. *Id.* This individual was confirmed to be Ms. Koehler. *Id.*

Fearing alerting the occupants without further information, the officers used a Doppler Radar to scan the main house and the pool house. *Id.* Doppler Radars rely on radio waves that detect movements up to 50 feet away. *Id.* It can zero in on a person's breathing, which makes it almost impossible to avoid detection while within range. *Id.* While these devices are very popular with the police, they have almost no public use. R. at 33. The main house scan revealed one person was inside; the pool house scan revealed one person pacing and three people being still. R. at 4.

The officers left and, based on their observations from the drone and Doppler radar, obtained a search warrant for the entire residence. R. at 46. Around 8:00 A.M., the officers returned to Macklin Manor with a SWAT team. R. at 5. Pursuant to the warrant, the SWAT team conducted a no-knock and notice, and entered the home and pool house. *Id.* They arrested multiple individuals, including Ms. Koehler, and found the three individuals who had been missing tied up. *Id.*

On October 1, 2016, Ms. Koehler was charged by indictment with three counts of kidnapping under 18 U.S.C § 1201(a) and one count of being a felon in possession of a handgun under 18 U.S.C. § 922(g)(1). *Id.* Then, in the United States District Court of the Southern District of Pawndale, Ms. Koehler filed a motion to suppress evidence seized on the date of her initial arrest on August 17, 2016, pursuant to Rule 12(b)(3)(c) of the Federal Rules of Criminal Procedure. *Id.* The District Court denied Defendant's motion to suppress evidence as obtained in violation of the Fourth Amendment. R. at 15.

Ms. Koehler appealed to the United States Court of Appeals for the Thirteenth Circuit on July 10, 2017. *Id.* Ms. Koehler appealed her conviction after guilty plea on charges of kidnapping and possession of a firearm by a felon, and she reserved her right to appeal the district court's ruling on her suppression motion. *Id.* Ms. Koehler contended the District Court erred in denying her motion to suppress evidence prior to her plea, and the Thirteenth Circuit agreed with Ms. Koehler and reversed the judgment entered against her, and remanded the case for further proceedings. R. at 21.

Petitioner then filed for Certiorari with the United States Supreme Court, which issued Petitioner a Writ of Certiorari, for its November 2017 term. R. at 22.

SUMMARY OF THE ARGUMENT

I. The Thirteenth Circuit's decision to reverse the District Court's denial of Ms. Koehler's Motion to Suppress, finding Agent Ludgate without reasonable suspicion conducted a non-routine search of Ms. Koehler's laptop, should be affirmed for two reasons. First, this Court should find that the intrusive and continued search of Ms. Koehler's laptop was a non-routine electronic data border search. This Court has ruled that electronic data

storage devices require greater protections based on sheer amount of qualitative personal information contained in these devices. A natural extension of *Riley* would be determine that searches of electronic devices are non-routine and require reasonable suspicion to insure individuals' Fourth Amendment rights are protected. For this reason, Agent Ludgate conducted a non-routine search on Ms. Koehler's laptop when she opened the laptop and continued looking through the files until she found what she needed. Otherwise, border officers could go through vast amounts of immensely personal data without any reason needed to justify their invasions of privacy, which would be extremely intrusive and unnecessary. Second, Officer Ludgate did not have reasonable suspicion to search Ms. Koehler's laptop. Reasonable suspicion is a particularized and objective basis for suspecting the particular person stopped of criminal activity. Officer Ludgate did not observe anything concerning Mr. Wyatt or the car that served as a basis for her suspecting Mr. Wyatt or Ms. Koehler stopped of criminal activity. Therefore, this Court should affirm the Thirteenth Circuit's decision reversing the District Court's denial of Ms. Koehler's Motion to Suppress because Officer Ludgate without reasonable suspicion performed a non-routine search of Ms. Koehler's laptop.

II. The Thirteenth Circuit's decision to reverse the District Court's denial of Petitioner's Motion to Supress should be affirmed. First, homes and their curtilages are granted heightened protections under the Fourth Amendment. Under *Dunn*, the pool and pool house are within the curtilage, because of their 15-50 foot proximity, their remote and negligibly visible location, and their use for home recreation. Second, the use of the PNR-1 drone amounted to an unreasonable search that violated the Fourth Amendment. Unlike this Court's past aerial surveillance cases, the drone was not the plain view

observation of an area regularly exposed to air travel. Further, applying these precedents directly to drone technology would lead to a significant erosion of privacy rights in society. Third, the use of the Doppler Radar also violated the Constitution. Using this Court's decision in *Kyllo*, it is clear that the use of the radar, which is not regularly used by the public, to view the otherwise hidden movements of people within a building, amounts to an unreasonable search. Additionally, the warrantless use of the radar did not promote any governmental interests, such as police safety, because the police ultimately left to retrieve a warrant anyway.

STANDARD OF REVIEW

Whether a warrantless search or seizure violated the Fourth Amendment is usually a question of law, requiring a de novo standard of review. *United States v. Montilla*, 928 F.2d 583, 588 n.2 (2d Cir. 1991).

ARGUMENT

I. THIS COURT SHOULD AFFIRM THE THIRTEENTH CIRCUIT'S DECISION BECAUSE THE OFFICER LUDWIG, WITHOUT REASONABLE SUSPICION, CONDUCTED A NON-ROUTINE SEARCH OF MS. KOEHLER'S PERSONAL LAPTOP IN VIOLATION OF HER FOURTH AMENDMENT RIGHTS.

The Thirteenth Circuit's ruling should be affirmed because the officers conducted a non-routine electronic data search through the files on Ms. Koehler's laptop without reasonable suspicion, which violated Ms. Koehler's Fourth Amendment rights.

The Fourth Amendment protects citizens against the violation of the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. This Court "has determined that warrantless searches and seizures are per se unreasonable unless they fall within a few narrowly defined exceptions." *Coolidge v. New*

Hampshire, 403 U.S. 443, 454-55, (1977). "The border search doctrine is a narrow exception to the Fourth Amendment prohibition against warrantless searches without probable cause." United States v. Sutter, 340 F.3d 1022, 1025 (9th Cir. 2003). In *United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008), the court declined "the government's invitation to decide th[e] case by holding that, at the border, anything goes."

Border searches are divided into two categories: routine and non-routine. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985). When crossing an international border into the U.S., a routine search does not require reasonable suspicion. *See generally United States v. Ramsey*, 431 U.S. 606 (1977) (involving customs mail inspection). Traditionally, non-routine border searches have been divided into two categories: an intrusive search of a person or a destructive search of property. *See Montoya de Hernandez*, 473 U.S. at 531*; United States v. Flores-Montano*, 541 U.S. 149, 124 S. Ct. 1582 (2004). This Court has not dealt directly with the world of digital information being searched at a border; however, in *Riley v. California*, this court decided that the immense storage capacity of cell phones that contains a digital record of nearly every aspect of the owner's life because "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person." 134 S. Ct. 2473, 2478 (2014). A cell phone is essentially a mini-computer and is "not just a physical object containing information." *Id*. "It is more personal than a purse or a wallet . . . . It is the combined footprint of what has been occurring socially, economically, personally, psychologically, spiritually and sometimes even sexually, in the owner's life." *Id*. A laptop computer contains even more information than a cell phone, and these facts do not change at the border; thus, this court should extend its ruling in *Riley* to require an officer to have reasonable suspicion before conducting a non-routine border search of electronic data. *See id*.

Reasonable suspicion is "a particularized and objective basis for suspecting the particular person stopped of criminal activity." *United States v. Cortez*, 449 U.S. 411, 417-18, (1981). Criminal activity includes "a crime [that] had just been, was being, or was about to be committed." *Brown v. Texas*, 443 U.S. 47, 51, (1979). This calculation is formed considering "the totality of the circumstances." *Cortez*, 449 U.S. at 417. "[E]ven when factors considered in isolation from each other are susceptible to an innocent explanation, they may collectively amount to a reasonable suspicion." *United States v. Berber-Tinoco*, 510 F.3d 1083, 1087 (9th Cir. 2007).

"Reasonable suspicion determinations are reviewed de novo, reviewing findings of historical fact for clear error and giving 'due weight to inferences drawn from those facts by resident judges and local law enforcement officers.'" *Ornelas v. United States*, 517 U.S. 690, 699, 116 S. Ct. 1657, 134 L. Ed. 2d 911 (1996) quoted in *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013).

Officer Ludgate's search was a non-routine search because she continued to look through all the files on Ms. Koehler's laptop until she was satisfied that she found all the information that she needed. R. at 2–3. This intrusive invasion of Ms. Koehler's subjective expectation of privacy of her laptop which contained all the privacies of her life is more intrusive than a strip search and required officer Ludgate to have reasonable suspicion before searching Ms. Koehler's laptop. R. at 3. None of the facts concerning Mr. Wyatt or the contents in the car seriously suggests that Officer Ludgate had the requisite reasonable suspicion to search the laptop. R. at 2. Further, Ms. Koehler's laptop contained hundreds if not thousands of files containing all aspects of her private life, which should not have been treated like an all-you-can-eat buffet for Agent Ludgate and the

government. R. at 2–3. Thus, this Court should find that this search was a non-routine electronic data search and Officer Ludgate did not have reasonable suspicion.

A. The Intrusive And Continued Search Of Ms. Koehler's Laptop Was A Non-Routine Search.

This Court has not decided what renders a border search non-routine for devices storing electronic data; furthermore, circuit courts are split between treating all searches of electronic data as routine and treating electronic data searches as non-routine searches requiring reasonable suspicion. *See, e.g., United States v. Stewart*, 729 F.3d 517, 526 (6th Cir. 2013); *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006). "In this regard, circuit courts have consistently held that searches of an individual's outer clothing, luggage, and personal effects are routine searches, whereas more physically intrusive searches—such as strip searches, alimentary canal searches, x-rays, and the removal of an artificial limb—are nonroutine searches requiring particularized reasonable suspicion." "The uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property." *Cotterman*, 709 F.3d at 966. Yet, this Court has not been clear about whether a search of electronic devices, such as laptops, is a routine or non-routine search. *See United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005) (finding that a manual search of electronic files located on a computer is the same as a manual search of papers contained in luggage, which is a typical example of a routine border search.) Thus, a clear rule finding Officer Ludgate's search of Ms. Koehler's laptop to be a non-routine search would not only follow the current circuit court trend of protecting private information on electronic devices, but it would also create a clear rule that protects all people's Fourth Amendment right of privacy.

In *Cotterman*, the court found a forensic probe into the defendant's laptop to be "essentially a computer strip search." 709 F.3d 952. In an 8-3 ruling, the Ninth Circuit held that

agents must have “reasonable suspicion” before they can conduct a “thorough and detailed search of the most intimate details of one's life” contained within digital devices. *Id.* The Ninth Circuit determined that the sheer amount of digital information contained within a laptop must be protected and is protected under the Fourth Amendment and found the search of the laptop to be a non-routine search requiring reasonable suspicion. *Id.* at 970.

Further, massive quantities of data produced by border searches reveal the almost unlimited ability of officers to go through millions of personal files; for example, in *United States v. Kim*, the D.C. Circuit held that a warrantless search of a laptop computer, seized before the defendant boarded the plane, "was supported by so little suspicion of ongoing or imminent criminal activity, and was so invasive of [defendant's] privacy," that it violated the Fourth Amendment. 103 F. Supp. 3d 32, 59 (D.D.C. 2015).

The DC Circuit, in *Kim*, granted the defendant’s motion to suppress evidence finding that the search “under the totality of the unique circumstances . . . was so invasive of Kim's privacy and so disconnected from not only the considerations underlying the breadth of the government's authority to search at the border, but also the border itself, that it was unreasonable.” 103 F. Supp. 3d 32, 59 (D.D.C. 2015). Logically, it follows that under the totality of the circumstances test, the level of invasiveness determines if the search is reasonable. *Kim* is controlling. Just as in *Kim* where the agents searched “the entire contents of Kim's laptop” for an “unlimited duration” and “unlimited scope[] for the purpose of gathering evidence in a pre-existing investigation” was a non-routine search, here, Agent Ludgate opened and searched Ms. Koehler’s laptop until she found the information she wanted without any limited duration or scope to the search. R. at 2–3. Therefore, Agent Ludgate’s search of Ms. Koehler’s laptop was a non-routine border search.

Petitioner may attempt to argue that *Kim* is distinguishable based on the high level of intrusiveness and unlimited duration of the search by the agents conducting the search of Kim's laptop; however, this argument misses the point of the case, which was not to provide a clear bright line for the level of intrusion needed, but was to protect Kim's right to privacy against any unreasonable searches. *See Kim*, 103 F. Supp. 3d at 59 (D.D.C. 2015). The D.C. Circuit followed the reasoning "utilized in *Riley*" and proceeded "by assessing, on the one hand, the degree to which [the search] intrudes upon an individual's privacy, and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id*. at 55 (internal citations omitted).

Kim and Ms. Koehler are similar because both stored vast amounts of personal information on their laptops with the expectation that the information would remain private and both of their laptops were subject to searches of unlimited scope and unlimited duration at the hands of boarder agents. *Id*. at 59; R. at 2–3. It is for these reasons that this Court should find that Agent Ludgate conducted a non-routine border search of Ms. Koehler's laptop.

B. Agent Ludgate Did Not Have Reasonable Suspicion To Search Ms. Koehler's Laptop.

"Reasonable suspicion exists when a law enforcement officer has specific and articulable facts, which, considered together with rational inferences from those facts, indicate that criminal activity may be afoot. *United States v. Hassanshahi*, 75 F. Supp. 3d 101, 119 (D.D.C. 2014) (internal citations omitted). Reasonable suspicion is "a particularized and objective basis for suspecting the particular person stopped of criminal activity." *Cortez*, 449 U.S. at 417-18. Criminal activity includes "a crime [that] had just been, was being, or was about to be committed." *Brown*, 443 U.S. at 51. This calculation is formed considering "the totality of the

circumstances." *Cortez*, 449 U.S. at 417. "[E]ven when factors considered in isolation from each other are susceptible to an innocent explanation, they may collectively amount to a reasonable suspicion." *Berber-Tinoco*, 510 F.3d at 1087. The totality of the circumstances reveals that Agent Ludgate did not have reasonable suspicion because she had no particularized or objective reason to suspect the seizure and search of Ms. Koehler's laptop stopped any criminal activity. R. at 2–3.

In *Cotterman*, the court deemed a forensic probe into the defendant's laptop "essentially a computer strip search" and held that agents must have "reasonable suspicion" before they can conduct a "thorough and detailed search of the most intimate details of one's life" contained within digital devices. 709 F.3d at 966. The court reasoned that "[t]he uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property." *Id*. In *Cotterman*, the Ninth Circuit ruled that defendant's prior child-related conviction, TECS alert, crossing from a country known for sex tourism, frequent travels, and collection of electronic equipment, plus the parameters of the Operation Angel Watch program, taken collectively, gave rise to reasonable suspicion of criminal activity. *Id*. at 956. *Cotterman* illustrates the importance of protecting the Fourth Amendment rights of individuals crossing the border, and the non-routine search of Ms. Koehler's laptop taken reveals that, unlike in *Cotterman*, the facts linking any possible criminal activity in any objective manner to Ms. Koehler's laptop are lacking. R. at 2–3.

While the reasonable suspicion requirement found in *Cotterman* is applicable, the amount of suspicious evidence is distinguishable. Ms. Koehler, unlike *Cotterman*, was not present when her laptop was seized, her past criminal offenses where not related to the internet or to her

laptop, and she did not have a collection of electronic equipment. R. at 2–3. In *Cotterman*, Cotterman's prior child-related conviction, TECS alert, crossing from a country known for sex tourism, frequent travels, and collection of electronic equipment, plus the parameters of the Operation Angel Watch program taken together gave rise to reasonable suspicion to search his laptop for child pornography; however, here, Ms. Koehler was a felon with multiple convictions for crimes of violence, not crimes utilizing a laptop, and named as a person of interest in the recent kidnappings. R. at 2. Neither of these two facts about Ms. Koehler come close to the six suspicious factors that created the requisite reasonable suspicion in *Cotterman*. Even considering Mr. Wyatt's agitated and uncooperative and the $10,000 in $20 bills in the trunk, these circumstances combined with Ms. Koehler's history fail to create "a particularized and objective basis for suspecting the particular person stopped of criminal activity." R. at 2; 449 U.S. at 417–18.

Petitioner may attempt to rely on *United States v. Feiten*, No. 15-20631, 2016 U.S. Dist. LEXIS 30331, at 5-6 (E.D. Mich. Mar. 9, 2016) to argue that laptop searches are routine searches that do not require reasonable suspicion, but *Feiten* is distinguishable and fails to protect individuals' Fourth Amendment rights. In *Feiten*, the court found that "[t]he Sixth Circuit has held that a 'routine border search of a laptop computer' does not require any level of suspicion, even when the computer 'is transported . . . beyond the border.'" *Id.* at 5 (quoting *United States v. Stewart*, 729 F.3d 517, 525 (6th Cir. 2013)). The defendant in Feiten attempted to argue that *Riley* meant that all searches of electronic devices required a warrant supported by probable cause, but the court stated that "*Riley* did not generate a blanket rule applicable to any data search of any electronic device in any context." *Feiten*, No. 15-20631, 2016 U.S. Dist. LEXIS 30331, at 12. The court found that "[l]aptops and cell phones are indeed becoming quantitatively,

and perhaps qualitatively, different from other items, but that simply means there is more room to hide digital contraband, and therefore more storage space that must be searched. *Id*. at 17.

Feiten is distinguishable. First, *Feiten* is a child pornography case, and "Customs officials are authorized to prevent the importation of contraband images and videos across the international border. To do so effectively, it is necessary to search entrants' electronic devices as most child pornography crimes involve use of a computer." *Id*. at 18. Unlike Feiten who had a record of frequenting destinations known for child sex tourism, Ms. Koehler was not linked to any crimes that utilized the internet and a laptop. R. at 2-3. Unlike the agents in Feiten who "had at least 178 valid reasons to suspect that more contraband might be contained [in his laptop]," Agent Ludgate knew only that the initials "AK" were on the laptop, which was not a valid reason to reasonably suspect that any contraband might be contained on Ms. Koehler's laptop. *Feiten*, No. 15-20631, 2016 U.S. Dist. LEXIS 30331, at 21; R. at 2.

It is for all the foregoing reasons that this Court should find that Agent Ludwig without reasonable suspicion performed a non-routine search of Ms. Koehler's laptop.

II. THE FOURTEENTH CIRCUIT SHOULD BE AFFIRMED BECAUSE THE STATE USE OF THE PNR-1 DRONE AND DOPPLER RADAR TO SURVEY THE CURTILAGE OF MS. KOEHLER'S HOME VIOLATED MS. KOEHLER'S REASONABLE EXPECTATION OF PRIVACY

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. At its most fundamental level, this Amendment protects a person's "constitutionally protected reasonable expectation of privacy." *Katz v. United States*, 389 U.S. 347, 360 (1967)

(Harlan, J., concurring); *see also California v. Ciraolo*, 476 U.S. 207, 211 (1986) (describing whether a person has a reasonable expectation of privacy as the "touchstone of Fourth Amendment analysis"). To determine whether such a reasonable expectation of privacy exists, this Court has established a two-prong test: 1. whether the individual manifested a subjective expectation of privacy in the object of the challenged search, and 2. whether society willing to recognize that expectation as reasonable. *Katz*, 389 U.S. at 361; *see e.g., Smith v. Maryland*, 442 U.S. 735, 740 (1979) (applying this test); *Rakas v. Illinois*, 439 U.S. 128, 143 (1978) (same).

At the "very core" of the Fourth Amendment's protection lies the right of a person to "be free from unreasonable government intrusion" within "his own home." *Silverman v. United States*, 365 U.S. 505, 511 (1961); *see* U.S. CONST. amend. IV (noting explicitly the people's right be secure in their "houses"). Thus, an individual's reasonable expectation of privacy is strongest in her home and its surrounding area. *See New York v. Burger*, 482 U.S. 691, 700 (1987); *Ciraolo*, 476 U.S. at 212-213 (1986). In contrast, there is no reasonable expectation of privacy for those things left in "open fields," *Hester v. United States*, 265 U.S. 57, 59 (1924), or readily available to the public view. *Dow Chem. Co. v. United States*, 476 U.S. 227, 239 (1986).

A. This Court's Precedent Indicates Ms. Koehler's Pool House And Pool Area Fall Within The Heightened Privacy Protections Of The Home

This Court has continually acknowledged that a person's Fourth Amendment interest does not stop at the physical walls of the home, but extends to areas "intimately linked to the home," which are encompassed in an area called the curtilage. *Ciraolo*, 476 U.S. 207, 213 (1986). To differentiate what is within this "curtilage" from what is in an "open field," this Court has proffered a four-prong test: 1. the proximity of the area to the home, 2. whether the area was included within an enclosure surrounding the home, 3. the nature of use to which the

area was put, and 4. the steps taken to protect the area from observation by people passing by. *United States v. Dunn*, 480 U.S. 294, 299 (1987).

In *Dunn*, a barn was held to be outside of the curtilage of a home. As to proximity, the barn was a lengthy sixty yards away from the house. *But see United States v. Breza*, 308 F.3d 430 (4th Cir. 2002) (finding a garden's fifty foot distance from house "would permit" conclusion garden was within curtilage). As to inclusion within the home's enclosure, the barn was not within the fence that surrounded the home. *But see United States v. Diehl*, 276 F.3d 32 (1st Cir.2002) (noting it the area was already naturally enclosed by forest). As to nature of use, the police had images of chemical containers being loaded into the barn, which was "objective data" that the barn was not being used for intimate activities of the home. *But see United States v. Jenkins*, 124 F.3d 768, 772 (6th Cir. 1997) (finding backyard within curtilage because it contained a garden and area for laundry to dry). As to protections, the Defendant had done little to protect the barn from observation. *But see Jenkins*, 124 F.3d at 773 (finding backyard within curtilage, because it was "well shielded" from those on public road by woods). Thus, all four factors disfavored inclusion of the barn into the curtilage.

Here, the pool and pool house appear to fall within the home's curtilage. Like *Breza*, where a distance of fifty feet would permit a finding an area was within the curtilage, here the distance of 15-50 feet also would permit such a finding. R. at 32. Like *Diehl*, where a forest created a natural enclosure, here the near perpetual fog and presence on a remote mountaintop created a natural enclosure blocking view from the public. R. at 3. Indeed, like in *Jenkins*, the distant location from town and thick fog prevent both average citizens and planes from regularly observing the home. *Id.* Lastly, like *Jenkins*, where the presence of a garden and laundry area amounted to a place where intimate activities of the home were performed, here the pool is a

place where people regularly recreate and enjoy the lack of external observation. *See Id.; Florida v. Riley*, 488 U.S. 445, 454 (1989) (J. O'Connor, concurring) (noting the legitimate social value of "enjoyment" of "outdoor patios and yards"). Thus, the pool and pool house likely fall within the home's heightened Fourth Amendment protections.

B. The Use Of The PNR-1 Drone Was A Search That Violated Ms. Koehler's Reasonable Expectation Of Privacy In Her Home

a. This Court's prior approvals of aerial surveillance are strongly distinguishable to the facts of this case.

It is the long-held precedent of this Court that "warrantless searches" are "presumptively unreasonable." *United States v. Karo*, 468 U.S. 705, 717 (1984). That being said, under certain circumstances, this Court has approved warrantless surveillance of portions of a home which are in "plain public view," under the reasoning that simple "visual observation is no 'search' at all." *Kyllo v. United States*, 533 U.S. 27, 32 (2001). Indeed, twice in the 1980s, this Court held law enforcement agents' naked eye surveillance of a home's curtilage from an aircraft to not be in violation of the Fourth Amendment. *See Florida v. Riley*, 488 U.S. 445 (1989); *Ciraolo v. California*, 476 U.S. 207, 215 (1986); *see also Dow Chem. Co. v. United States*, 476 U.S. 227 (1986) (holding aerial photography of open areas of an industrial complex did not violate the Fourth Amendment). In comparison to the instant case, however, it is readily apparent that the facts of *Ciraolo* and *Riley* are strongly distinguishable.

First, in *Ciraolo v. California*, this Court found that there was no reasonable expectation of privacy in an individual's backyard when it was "visible to the naked eye" from a plane at 1000 feet. 476 U.S. 207, 215 (1986). There, the police received an anonymous tip that Defendant was illegally growing marijuana in the backyard of his suburban home. *Id.* However, a six-foot outer fence and a ten-foot inner fence completely prevented the police from observing

the backyard. *Id.* Consequently, the police chartered a plane and flew over the house at a legally permissible altitude of 1000 feet. *Id.*at 216. Passing over the home, the investigating officers "readily identified" marijuana plants approximately 8-10 feet tall. *Id.*Based on their "naked-eye" observation and the pictures, the officers were granted a warrant to seize the marijuana. Reviewing the constitutionality of the warrant, the Court applied the two-part inquiry from its decision in Katz. *Id.*at 217. As to the subjective expectation of privacy in the backyard, the Court recognized "that the 10-foot fence was placed to conceal the marijuana crop from at least street-level views." *Id.* at 211. However, because a citizen or police officer likely could have seen the marijuana from "the top of a truck or a two-level bus," it was "not entirely clear" that the Defendant possessed a "subjective expectation of all observations." *Id.* As to society's willingness to view the expectation as reasonable, the Court evaluated whether the surveillance violated "the personal and societal values protected by the Fourth Amendment." *Id.* at 212 (quoting Oliver, 466 U.S., at 181-183). Although the backyard was indisputably within the curtilage of the home, the "Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares." *Id.*at 211. It was likely that any "member of the public flying in this airspace who glanced down could have seen everything that these officers observed," especially in "an age where private and commercial flight is routine." Id at 213. Lastly, the Court rejected warnings from *Katz* that "electronic developments" could erode privacy rights, because those warnings were not aimed at "simple visual observations from a public place." *Id.* Ultimately, there was no reasonable expectation of privacy because one is not "entitled to assume his unlawful conduct will not be observed by a passing aircraft-or by a power company repair mechanic on a pole overlooking the yard." *Id.* at 214-15 (quotes omitted).

Ciraolo is distinguishable from the case at hand. Unlike *Ciraolo*, where the government used naked eye surveillance of the property, the government here used a sophisticated piece of technology, equipped with a high definition camera and video taking capabilities. R. at 32. Further, dissimilar to *Ciraolo*, where anyone on a routine flight over the property could have seen the marijuana, the severe, year-round fog and clouds caused airplanes to "steer clear of flying over Mount Partridge." R. at 3. On the day in question, the police even noted that it was very low visibility, such that they did not see or hear any aircraft, and even the drone had difficulties from the fog. R. at 32. Perhaps even more drastically, unlike *Ciraolo*, where the evidence could have been observed by a person on a bus or a worker on a telephone pole, here, the property is at "the outskirts of town," and is literally on top of a mountain, and it is very unlikely that any average citizen would be in a position to see what the government observed. Lastly, unlike *Ciraolo*, where the warnings in Katz about electronic surveillance were disregarded because they did not concern a "simple visual search," here, there does not seem to be anything simple about the visual search in this case. This surveillance required a $4000 piece of machinery flying, specifically designed for police usage, hovering for 15 minutes over an area, while the "pilot" is watching from another location. R. at 32, 38. As such, the reasoning that "police should not have to close their eyes" when passing through "public thoroughfares" does not apply because the airspace above the home does not receive enough traffic to be remotely considered a thoroughfare, meaning Ms. Koehler would reasonably expect her home to exposed to such investigation.

Second, in *Florida v. Riley*, a plurality of this Court found that the "naked-eye" viewing through the hole in a greenhouse from a helicopter flying at 400 feet did not violate the Fourth Amendment. 488 U.S. 445, 454 (1989). In that case, the police received a tip that the Defendant

was growing marijuana on his property. *Id.* Because he could not see the contents of property's greenhouse from the road, a police officer "circled twice over [Defendant's] property in a helicopter at the height of 400 feet. *Id.* "With his naked eye," the officer could see through the openings in the roof and sides of the greenhouse and "identify what he thought was marijuana growing in the structure." *Id.* Based on this observation, the police were able to receive a search warrant. Id at 457. Analyzing subjective expectation of privacy, the four-justice plurality opinion noted that "the sides and roof of his greenhouse were left partially open." *Id.* Further, "helicopters flying in the public airways is routine in this country," and it was not "unheard of" for helicopters to fly in the area. *Id.* Thus, the defendant would have known that "what was growing in the greenhouse was subject to viewing from the air." *Id.*at 460. As to the reasonableness of the defendant's expectation, the Court noted aerial surveillance will not always "pass muster" purely because the vehicle was "within the navigable airspace specified by law." *Id.*at 461. However, the Court stated, in this case, defendant's expectation of privacy was not reasonable because "any member of the public could legally have been flying over *Riley*'s property in a helicopter at the altitude of 400 feet and could have observed *Riley*'s greenhouse." *Id.* Additionally, there was no evidence that the surveillance "interfered with respondent's normal use of . . . the curtilage." *Id.* Thus, the Court affirmed surveillance. While agreeing with this outcome, Justice O'Connor's concurrence criticized the plurality's emphasis on the fact that the helicopter was legally permitted to fly in that airspace. *Id.*at 462. While, in this case, there was "considerable use of the public airways," in other cases, the use of certain airspaces "may be sufficiently rare that police surveillance from such altitudes would violate reasonable expectations of privacy." *Id.*

The instant case is also distinguishable from *Riley*. Whereas in *Riley*, where helicopter flights were not unheard of for the area, planes actually steer clear of the area above Ms. Koehler's home. R. at 3. Thus, the case at hand appears to satisfy Justice O'Connor's consideration that places where air travel is possible, but rare, can still lead to a reasonable expectation of privacy. Importantly, no flights were actually seen or heard that day, leaving Ms. Koehler with an actual belief that no one was surveilling her. R. at 42. Further, unlike *Riley*, where the helicopter was always in it legal airspace, the drone here likely was not. Indeed, there was a 4-5 minute period where the government lost track of the drone and "there is no way of telling whether the drone exceeded the 1640 feet limit" as they had done 60% in the past. R. at 41. While the altitude limit was intended to prevent collision with airplanes, exceeding that limit could make an already "discreet" device much harder to see, especially at dawn when the surveillance occurred. R. at 3, 46. Additionally, dissimilar to *Riley*, where a plain-view observation occurred while a helicopter circled twice over the greenhouse, the drone hovered over the home for 15 minutes while taking high definition pictures and multiple minutes of video. R. at 4.

b. Because of the rapid proliferation of drone technology, reversing the Fourteenth Circuit would lead to a significant erosion of privacy rights

The immediate case is the first time this Court is dealing with the implications of drone technology on the Fourth Amendment, and consequently, the "question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). This Court has long recognized that new technology often brings the danger of diminished privacy rights. *United States v. Jones*, 565 U.S. 400, 427 (2012) (J. Kagan, concurring) ("New technology may provide increased

convenience or security at the expense of privacy. . . ."). Accordingly, it has recognized that its precedent-creating decisions must be made with an eye to the potential development of greater technological advancement. *Kyllo*, 533 U.S. at 2044 ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."). In fact, where prior opinions did not properly forecast current technology, this Court has declined to extend its own precedent to "technology nearly inconceivable" to the past Justices. *Riley v. California*, 134 S. Ct. 2473 (2014) (refusing to extend the Court's decades long "search incident to an arrest" precedent to the realm of cell phones); *Katz*, 389 U.S. 347, 362 (1967) (rejecting a prior case because it was "bad physics as well as bad law, for reasonable expectations of privacy may [now] be defeated by electronic as well as physical invasion.").

This Court should similarly be hesitant to apply its precedent to drones, which are indeed such a technology that has the power "to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34. Drone technology is rapidly growing and will continue to grow within the country, with an estimated thirty thousand non-military drones operating in the U.S. by 2030. Matthew R. Koerner, *Drones and the Fourth Amendment: Redefining Expectations of Privacy*, 64 DUKE L.J. 1129, 1149 (2015). The use of these flying devices already spans the spectrum of industries—from farming, to border patrol, to pizza delivery—and it is expected that their prevalence will only further integrate into daily life. *Id.* Further, examining "the more sophisticated systems that are already in use or in development," *Kyllo*, 533 U.S. at 2044, some drones are equipped with the highest-powered cameras and other sense-enhancing devices, while others are designed to be imperceptibly small or to operate at an extremely high altitude. Koerner, 64 DUKE L.J. at 1149-51.

As the drones continue their dramatic growth in both use and sophistication, merely applying the current law, that individuals have no privacy in things easily seen from regularly used airspace, to drones could leave society with almost no places that are deemed private. *See Riley*, 488 U.S. at 453–54 (1989) (noting that "even individuals who have taken effective precautions to ensure against ground-level observations cannot block off all conceivable aerial views of their outdoor patios and yards without entirely giving up their enjoyment of those areas."). As such, numerous commentators have suggested that Fourth Amendment jurisprudence is inherently unfit for a direct application to drone technology. *See e.g.*, John Villasenor, *Observations from Above: Unmanned Aircraft Systems and Privacy*, 36 HARV. J.L. & PUB. POL'Y 457 (2013); Philip J. Hiltner, Comment, *The Drones Are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and Its Fourth Amendment Implications*, 3 WAKE FOREST J.L. & POL'Y 397 (2013).

C. The Use Of The Handheld Doppler Radar Is A Direct Contradiction Of This Court's Decision In *Kyllo*

In *Kyllo v. United States*, this Court held that warrantless use of thermal-imaging to show the inside of a home violated the Fourth Amendment. 533 U.S. at 34. There, a federal agent was suspicious that the defendant was growing marijuana inside of his home, and used the device to investigate whether defendant was utilizing heat lamps inside to grow the plants. *Id.* The scan showed certain areas of the home were substantially warmer than neighboring residences. *Id.* Based on this evidence, the police were granted a warrant to search the home. *Id.* Even though an onlooker could tell that one home was emitting greater heat by watching the rate of water evaporation or snow melting on the home, use of the sense-enhancing device amounted to a search because it permitted the officers to "explore details of the home that would previously have been unknowable without physical intrusion." *Id.* at 40. While the device only measured

heat, and not other more intimate details, "*all* details are intimate details" in an area "held safe from government eyes." *Id.*(emphasis original). Further, with a concern that advanced "police technology" would "erode the privacy guaranteed by the Fourth Amendment," the Court noted that lack of "routine" use by the general public cut against its warrantless use. *Id.* at 42.

This case is strongly analogous to *Kyllo*. Like *Kyllo*, where the use of the device was not in general public use, but has almost no general use by the public, with the police even conceding that there is not "any reason why the average citizen would own one." R. at 35. Similar to *Kyllo*, which drew a distinction between "police technology" and that in "general public use," the fact that Doppler Radars are supposedly "super popular" with police does not equate to satisfying the general public use prong of the *Kyllo* test. R. at 33. Indeed, while this technology is relatively new, the only published federal case that has dealt Doppler Radar, United States v. Denson, 775 F.3d 1214, 1218 (10th Cir. 2014) (J. Gorsuch), noted "the government's warrantless use of such a powerful tool to search inside homes poses grave Fourth Amendment questions." Further, like *Kyllo*, where the thermal imaging permitted the officers to see the marijuana lamps which would otherwise require intrusion into the home, here the Doppler Radar allowed the police to see the movements and even the breaths of the inhabitants of the home and the pool house. R. at 4. Like *Kyllo*, which rejected the thermal device even though an onlooked could have seen certain parts of the home were warmer because of snow melt or water condensation, the mere fact that the police could have gathered similar information by watching the number of people that come or go is not dispositive here. *See* R. at 11.

Lastly, permitting the use of the Doppler Radar in this instance does not provide a "workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment." *Oliver*, 466 U.S. at 171. While such a device may assist promoting the

safety of police officers, a legitimate governmental interest, the warrantless use of the device did not promote safety in this case. Notably, after using both the drone and the Doppler device, the officers left to retrieve a warrant and returned later to search the home. As such, the device would have been just as effective in detailing the number of inhabitants had the police waited until they had a warrant. R. at 35. While there may be an instance where the warrantless use of such technology is appropriate, this is certainly not that case.

For the foregoing reasons, this Court should affirm the Thirteenth Circuit's finding that the use of both the PNR-1 drone and the Doppler device violated the Fourth Amendment.

CONCLUSION

For the foregoing reasons, Mathison respectfully requests that the Court uphold the decision of the Thirteenth Circuit and hold that:

1. The search of Ms. Koehler's laptop was not valid pursuant to the border exception of the warrant requirement.
2. The use of the PNR-1 drone and the Doppler Radar amounted to unreasonable searches of Ms. Koehler's curtilage.

Dated: October 20, 2017 Respectfully submitted,

Team 14