Respondent Team 26

No. 4-422

IN THE
Supreme Court of the United States

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 the Respondent

Counsel for Respondent
October 20, 2017

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

United States Supreme Court

United States Courts of Appeals

United States District Courts

Statutes

Other Authority

ISSUES PRESENTED FOR REVIEW

I. Whether the Government's nonconsensual, warrantless search of Ms. Koehler's laptop at a border station violated her rights per the border exception to the warrant requirement of the Fourth Amendment.

II. Whether the Government's warrantless use of a drone to surveil an area with little to no air traffic, while violating Federal Aviation Administration regulations, and use of a Doppler radar device, not in general public use, to reveal the number and location of people within a building violated Ms. Koehler's Fourth Amendment right against unreasonable searches.

No. 4-422

IN THE
Supreme Court of the United States

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 the Respondent

STATEMENT OF FACTS

On August 17, 2016 at 3:00 a.m., Border Patrol Agents Dwyer and Ludgate stopped a car driven by Scott Wyatt at the Eagle City Border Station. R. at 2. The agents noticed that Mr. Wyatt was agitated and uncooperative when asked why he was entering the United States. R. at 2. Agent Ludgate then asked if Mr. Wyatt was carrying $10,000 or more in U.S. currency. R. at 2. He replied that he was not. R. at 2. Agent Ludgate informed Mr. Wyatt of their right to search his car, at which point he stepped out of the vehicle. R. at 2. When Mr. Wyatt opened the trunk, Agents Ludgate and Dwyer discovered $10,000 in cash along with a laptop with the initials "AK" engraved on the surface. R. at 2. When prompted, Mr. Wyatt told the agents that he shared the laptop with his fiancé, Respondent Amanda Koehler. R. at 2. The agents ran Ms. Koehler's name in a criminal database and discovered that she had a criminal history and was named as a person

of interest in the kidnapping of billionaire Timothy Ford's three children. R. at 2. The Ford children were kidnapped and held for ransom, but the kidnappers recently agreed to give Mr. Ford proof of life in exchange for $10,000, due at noon the next day. R. at 2. Aware of the investigation, Agent Ludgate opened Ms. Koehler's laptop and began searching through her files. R. at 2. She discovered files containing Mr. Ford's personal information and a lease agreement with the name "Laura Pope" for a property called "Macklin Manor." R. at 3. "Laura Pope" is an alias of Ms. Koehler. R. at 3. At that point, Agent Ludgate contacted Detective Perkins of the Eagle City Police Department ("ECPD"), the lead detective in the kidnapping investigation. R. at 3.

R.A.S.—a shell company owned by "Laura Pope"—purchased Macklin Manor around May of 2016. R. at 1, 3. Macklin Manor has been abandoned since 2015, and no residents have been seen there since. R. at 3. The property is on the outskirts of Eagle City atop Mount Partridge, an area that is perpetually cloudy and foggy. R. at 3. Due to the extremely limited visibility, aircraft routinely fly around the area rather than through it. R. at 3.

Around 4:30 a.m. that same morning, Detective Perkins and ECPD Officers Lowe and Hoffman arrived at Macklin Manor without a warrant. R. at 1, 3, 4. At dawn, Officer Hoffman conducted foot surveillance while Officer Lowe deployed a PNR-1 drone to fly over the property. R. at 3. PNR-1 drones are programmed with a maximum flight altitude of 1640 feet—the legal maximum in the state—but due to recent network connectivity errors, some units have flown as high as 2000 feet. R. at 4. The PNR-1 took photos and video that provided the layout of the property. R. at 4. Macklin Manor includes a main house, an open pool and patio area, as well as a pool house. R. at 4. The property is not gated or fenced. R. at 4. The pool is about fifteen feet from the main house, and the pool house is on the other side of the pool, about fifty feet from the

main house. R. at 4. The PNR-1 also photographed a single young female, later confirmed to be Ms. Koehler, crossing from the main house to the pool house. R. at 4

Detective Perkins and Officer Hoffman surreptitiously approached the front door area of the main house to scan it with a handheld Doppler radar. R. at 4. In recent years, handheld Doppler radars have become popular among law enforcement. R. at 4. These devices emit a radio wave that allow it to detect an individual's movements up to fifty feet inside of a building. R. at 4. They often "zero in" on a person's breathing to locate them. R. at 4. Although Doppler radars cannot reveal the interior layout of a building, they can reveal the number and rough locations of people inside. R. at 4. A scan of the main house revealed a person a few feet from the front door. R. at 5. The police continued to the pool house, and another scan revealed three people inside, close together and not moving, but still breathing. R. at 5. Nearby, another person appeared to be pacing around, presumably standing guard. R. at 5.

After the two radar scans, the police left. R. at 5. They returned around 8:00 a.m. the same morning with a SWAT team and a search warrant for the entire residence. R. at 5. The police conducted a no-knock and notice pursuant to the warrant and detained two people in the living room of the main house. R. at 5. Ms. Koehler ran out the back door, but was apprehended before she could leave the premises. R. at 5. The police seized a handgun from Ms. Koehler's person. R. at 5. The police then forcibly entered the pool house, detained the guard inside, and found the three Ford children restrained to chairs, but unharmed. R. at 5.

On October 1, 2016, Ms. Koehler was indicted on three counts of kidnapping and one count of being a felon in possession of a handgun. R. at 5. Ms. Koehler filed a motion to suppress the evidence, which was denied by the United States District Court for the Southern District of Pawndale on November 25, 2016. R. at 1. On appeal, the United States Court of Appeals for the

Thirteenth Circuit reversed and remanded on July 10, 2017. R. at 14-15. This Court granted certiorari. R. at 22.

SUMMARY OF ARGUMENT

Although Courts have recognized a lower expectation of privacy at the border, the search of Ms. Koehler's laptop at the Eagle City border station violated her Fourth Amendment rights because it was non-routine and lacked reasonable suspicion. The search was non-routine because it was exceedingly invasive and exposed Ms. Koehler's private documents. Also, while the agents had reasonable suspicion to search Mr. Wyatt's car, no reasonable suspicion existed to search Ms. Koehler's laptop. Finally, this Court has recognized the increased privacy risks involved in digital searches of cell phones, and this analysis should be applied to digital searches at the border as well.

Eagle City Police's warrantless drone and radar surveillance also violated Ms. Koehler's Fourth Amendment rights. Ms. Koehler has a reasonable expectation of privacy from drone surveillance of her property and the use of the PNR-1 drone constituted an illegal search. Ms. Koehler also has a reasonable expectation of privacy from her property being scanned by a Doppler radar device not in general public use which reveals information that would not have otherwise been obtainable without entering the home. Finally, the evidence obtained as a result of using the PNR-1 drone and the Doppler radar constitute fruits of the poisonous tree. Absent the illegal searches, there is no probable cause to support a search warrant.

STANDARD OF REVIEW

Questions of law are reviewed de novo. *Pierce v. Underwood*, 487 U.S. 552, 558 (1988). In the present case, both issues presented involve the application of the Fourth Amendment. Furthermore, this court has held that "ultimate questions of reasonable suspicion and probable cause to make a warrantless search should be reviewed de novo." *Ornelas v. United States*, 517

U.S. 690, 691 (1996). Whether police conduct is a "search" under the Fourth Amendment is a mixed question of law and fact, where de novo review is also appropriate. *United States v. Broadhurst*, 805 F.2d 849, 852 (9th Cir. 1986) (citing *United States v. McConney*, 728 F.2d 1195, 1203 (9th Cir.1984)). As such, the appropriate standard of review is de novo.

ARGUMENT

I. THE GOVERNMENT'S SEARCH OF MS. KOEHLER'S LAPTOP AT THE BORDER STATION WAS A NON-ROUTINE SEARCH FOR WHICH AGENTS LACKED REASONABLE SUSPICION.

This case involves the degradation of Ms. Koehler's Fourth Amendment rights. While the search of her laptop took place at the United States border, those circumstances did not permit the Government to acquire unrestricted access to her private digital files. The Fourth Amendment to the United States Constitution protects the right of individuals to be secure in their papers and effects against unreasonable searches and seizures. U.S. CONST. amend. IV. All warrantless searches are presumed to be unreasonable, unless the Government can establish that a recognized exception applies. *Katz v. United States*, 389 U.S. 347, 357 (1967). The border search exception to the Fourth Amendment gives the Government authority to conduct warrantless, suspicionless searches at the border because the Government's interest in protecting against the entry of unwanted persons and effects is "at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004); see also *United States v. Ramsey*, 431 U.S. 606, 616 (1977). However, border agents must have reasonable suspicion to conduct a more invasive, "non-routine" search. *United States v. Braks*, 842 F.2d 509, 511 (1st Cir. 1988).

This case involves the intersection of the border search exception with the search of a digital device. The development of technology has "shrunk the realm of guaranteed privacy" in modern society, and this Court has already recognized the privacy interests threatened by searches

of cell phones during searches incident to arrest and inventory searches. *Kyllo v. United* States, 533 U.S. 27, 34 (2001); *Riley v. California*, 134 S.Ct. 2473, 2475 (2014). This Court should require reasonable suspicion for searches of digital devices at the border.

A. The Search of Ms. Koehler's Laptop Was a Non-Routine Search Because It Was Unreasonably Invasive and Exposed a Multitude of Her Personal Files to the Prying Eyes of the Government.

The search of Ms. Koehler's laptop was non-routine because it invaded her privacy interests and placed her most private data in the hands of the Government. Routine searches are those that do not seriously invade an individual's right to privacy. *United States v. Johnson*, 991 F.2d 1287, 1291 (7th Cir. 1993). In contrast, non-routine searches require reasonable suspicion. *Braks*, 842 F.2d at 511. While a search of a border entrant's suitcase or overcoat is routine, body cavity and strip searches are non-routine. *Id.* In determining whether a search is routine or non-routine, courts balance the border agent's level of suspicion against the level of indignity perpetrated against a traveler. *United States v. Dorsey*, 641 F.2d 1213, 1219 (7th Cir. 1981).

In *United States v. Flores-Montano*, this Court held that warrantless, suspicionless searches of vehicles—including those that involve the removal, disassembly, and reassembly of a vehicle's fuel tank—are routine, and thus do not require reasonable suspicion. *United States v. Flores-Montano*, 541 U.S. 149 at 152. This Court noted that because smugglers frequently cross the border with contraband in their vehicles, a search of a gas tank, "which is solely used for fuel," is not an unreasonable violation of privacy. *Id.* at 154. Similarly, minimally intrusive tests designed to detect the presence of hidden contraband in a traveler's luggage are also routine because they do not harm the property, take only minutes, and do not involve any indignity to the traveler. *Johnson*, 991 F.2d at 1291-92.

On the other hand, this Court held that a detention of an individual at the border which goes "beyond the scope" of a routine customs interaction is justified if agents reasonably suspect that the traveler is smuggling narcotics in his or her alimentary canal. *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985). In *Montoya de Hernandez*, a woman suspected of such an offense was detained for nearly sixteen hours after she refused to submit to an x-ray of her torso, and instead opted to remain in detention while agents awaited her bowel movement. *Id.* at 543. This interaction went far beyond a "routine" search, and this Court aptly held that border agents must have reasonable suspicion in order to invade a traveler's privacy to such an intrusive extent. *Id.* at 541. Additionally, courts have consistently held that strip-searches and body cavity searches are non-routine border searches requiring reasonable suspicion. *Braks*, 842 F.2d at 512.

Here, border agents searched a laptop with the capacity to store a multitude of personal information; this is simply not analogous to the routine search of a vehicle's gas tank or that of a suitcase as in *Flores-Montano* and *Johnson*. Although the search of a digital device at the border is not intrusive in the same way a strip search, body cavity search, or x-ray is, it still involves an indignity that should not occur without reasonable suspicion. Also, the language from *Montoya de Hernandez* suggests that this Court's reasoning can and should be applied to different factual scenarios. Ms. Koehler's laptop contained records of her entire life in digital form, and her privacy was invaded simply because Agent Ludgate assumed she could rifle through the device as part of the search of Mr. Wyatt's vehicle. R. at 28. This reasoning cannot stand, and this Court should recognize a truth of modern society: digital devices contain footprints of our lives, and allowing the Government to intrude upon that information without reasonable suspicion would jeopardize Fourth Amendment protection at the border to a dangerous extent.

//

B. Agent Ludgate Did Not Have the Mandatory Reasonable Suspicion to Search Ms. Koehler's Laptop During the Border Stop.

1. The search lacked reasonable suspicion because Agent Ludgate failed to establish a particularized, objective basis for suspecting Ms. Koehler of wrongdoing.

Even taking into account Mr. Wyatt's nervous behavior and his relationship with Ms. Koehler, Agent Ludgate did not have reasonable suspicion to search the laptop because there was a lack of specific facts that suggested Ms. Koehler was engaged in criminal activity. When a border search becomes non-routine, a customs official needs reasonable suspicion to justify it. *Montoya de Hernandez*, 473 U.S. at 538. Reasonable suspicion is a "particularized and objective basis for suspecting [a] particular person" of engaging in criminal activity. *Id.* at 541. To establish reasonable suspicion, the Government must show "objective, articulable facts that justify the intrusion to the particular person and place searched." *Id.*; see also *United States v. Asbury*, 586 F.2d 973, 975 (2d Cir. 1978) (noting that a border agent's suspicions should be based on "more than the border crossing" itself). The degree of intrusion must be reasonably related in scope to the circumstances which justified it initially. *Montoya de Hernandez*, 473 U.S. at 542.

The Second Circuit enumerated several factors that courts may consider in making the determination of reasonable suspicion including "unusual conduct of the defendant, discovery of incriminating matter[s] during routine searches, computerized information showing propensity to commit relevant crimes, or a suspicious itinerary." *United States v. Irving*, 452 F.3d 110, 124 (2d Cir. 2006). The Fifth Circuit has also held that reasonable suspicion for a non-routine border search can also be established through corroboration of a tip. *United States v. Roberts*, 274 F. 3d 1007, 1012 (5th Cir. 2001). *Roberts* involved an anonymous tip that the defendant would be flying to France on a certain day carrying computer disks of child pornography in his shaving kit. *Id.*

The court held that if sufficient details of a tip are corroborated, "reasonable suspicion to conduct a non-routine border search is established." *Roberts*, 274 F. 3d at 1015.

In the present case, the border agents lacked specific, articulable facts that pointed to a showing of reasonable suspicion before they searched Ms. Koehler's laptop. Mr. Wyatt's nervousness coupled with the fact that his fiancé had a criminal record does not amount to reasonable suspicion. There was no corroborated tip suggesting Ms. Koehler's laptop contained evidence of an ongoing crime as in *Roberts*, and Mr. Wyatt's travel itinerary was not on its own suspicious. While Mr. Wyatt may have displayed "unusual behavior" consistent with the first *Irving* factor, the circumstances of the stop still fell short of establishing reasonable suspicion. Although Ms. Koehler had a criminal history, her past crimes did not involve the use of a digital device, and *Irving* suggested agents consider propensity to commit *relevant* crimes. *Irving*, 452 F.3d at 124. Furthermore, while Mr. Wyatt's failure to declare the $10,000 in U.S. currency could be considered an "incriminating matter," it did not directly suggest any wrongdoing on the part of Ms. Koehler, who was not even present during this border stop.

2. Agent Ludgate's authority to search Mr. Wyatt's vehicle did not give her authority to search the laptop.

The quantum of facts necessary to justify a particular search may not suffice to justify a more intrusive or demeaning search. *United States v. Afanador*, 567 F.2d 1325, 1328 (1978). Additionally, all searches that implicate the Fourth Amendment must conform with its "ultimate touchstone: reasonableness." *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). In *Montoya de Hernandez*, this Court reasoned that "the degree of intrusion must be reasonably related in scope to the circumstances which justified it initially." *Montoya de Hernandez*, 473 U.S. at 542.

In *Afanador*, officers were tipped off that a flight attendant traveling to Miami would be carrying cocaine on her person. *Afanador*, 567 F.2d at 1328. When the flight landed, officers

conducted strip searches of both the woman identified in the tip along with a second flight attendant with whom she was traveling. *Afanador*, 567 F.2d at 1328. The court held that the search of the second woman lacked reasonable suspicion, because while corroboration of the tip was attained with regard to the first woman, the same could not be said for the second. *Id.* Thus, reasonable suspicion established for one search does not automatically establish reasonable suspicion for a second, different search. *Id.* The reasonable suspicion test requires the Government to justify the intrusion for the *particular* search. *Id*.

Here, it was certainly reasonable for the border agents to do a routine search of Mr. Wyatt's car as is consistent with border search protocol. However, Agent Ludgate's search through the laptop was an extreme escalation of the initial border search of the vehicle. Also, Agent Ludgate admitted that she did not seek a warrant, despite having the "time to retrieve [one]," and assumed that "it was part of the search of the car." R. at 28. This demonstrates that she lacked reasonable suspicion to justify the intrusion into Ms. Koehler's laptop, and indicates that she misunderstood the Fourth Amendment as a whole. As such, this Court should affirm the lower court's ruling that "while there may have been reasonable suspicion to search [Mr. Wyatt's] car, there was no reasonable suspicion to search the laptop." R. at 17.

C. This Court Should Require Reasonable Suspicion for Digital Searches at the Border, and Hold that Agent Ludgate's Search Violated Ms. Koehler's Rights.

Under this Court's decision in *California v. Riley*, 134 S.Ct. 2473 (2014), Agent Ludgate infringed on Ms. Koehler's right to privacy in her papers and effects by searching her laptop without consent and without reasonable suspicion. The Fourth Amendment's protection of one's "papers" reflects our Founders' concerns with "safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the Government." *United States v. Seljan*, 547 F.3d 993, 999 (9th Cir. 2008). In *Riley*, this Court discussed the substantial privacy

interests implicated by the common use of digital devices by modern Americans, and the interaction of these interests with the Fourth Amendment. *Riley*, 134 S.Ct. at 2488.

Following that decision, scholars discussed how courts might address cases that involve an intersection of the border search exception with *Riley*'s protection of privacy in digital devices. One law review article summarized the issue as whether searches of electronic devices are seen "more like strip searches or . . . pat-downs." Matthew B. Kugler, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. Chi. L. Rev. 1165, 1176-77 (2014). Another article suggested that the authority to search a laptop at the border should depend on whether it is reasonable "to search for information that has little to do with customs laws at the border." Victoria Wilson, *Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States Borders from Bombs, Drugs, and the Pictures from Your Vacation*, 65 U. Miami L. Rev. 999, 1018-19 (2011).

1. This Court should resolve the circuit split concerning pre-*Riley* attempts to apply the border search doctrine to searches of digital devices.

The circuit courts have split in applying the border search doctrine to searches of digital devices. While some courts were reluctant to recognize any digital search as different from that of a suitcase or car, others acknowledged the unique privacy interests at stake. Still others attempt to draw distinctions between *types* of digital searches based on levels of intrusiveness.

The Fourth Circuit has held that border searches of laptops are routine. *United States v. Ickes*, 393 F.3d 501, 506-07 (4th Cir. 2005). In *Ickes*, agents searched the defendant's computer following their discovery of child pornography in his van during a routine stop. *Id.* The court rejected the defendant's argument that such a holding would subject any person carrying a laptop across a border to an invasive search of that device's hard drive. *Id.* The *Ickes* court doubted that

reality would manifest because border agents neither have the "time nor the resources" to search every traveler's laptop. *Id.*

In contrast, both the Second and Fifth Circuits suggested that searches of computer disks could be considered non-routine. While the courts in *Roberts* and *Irving* declined to decide whether the particular searches at issue in those cases were routine or non-routine—since border agents had reasonable suspicion in both—the language of these opinions suggests that such a search could be considered non-routine depending on the circumstances.

The Ninth Circuit attempted to deal with this issue by considering the intrusiveness of each particular search and ignoring storage capacity as a factor in the reasonable suspicion calculation. In 2008, the Ninth Circuit held that asking a traveler suspected of carrying child pornography to simply "boot up" his laptop was a routine border search, and stated that a device's storage capacity should not be a factor in determining the reasonableness of a search. *United States v. Arnold*, 523 F.3d 941, 947, 1010 (9th Cir. 2008). The court also distinguished between routine and non-routine digital searches by labeling *cursory* searches as routine and *forensic* searches as non-routine due to the deeper intrusion upon "personal privacy and dignity." *United States v. Cotterman*, 708 F.3d 952, 967 (9th Cir. 2013). In *Cotterman*, a border agent searched the defendant's laptop after learning he had a prior conviction for child molestation. *Id.* at 968. Nothing was found during the initial cursory search, but a comprehensive forensic search later revealed child pornography. *Id.*

This Court should create a clear rule for government agents at the border and require reasonable suspicion for every digital search. The Fourth Circuit was incorrect in evaluating their ruling based on whether the decision would impact *every* person crossing the border. This Court should recognize that each traveler has an individual expectation of privacy that must be respected. Further, the *Ickes* decision can remain intact because the agents in that case *did* possess reasonable

suspicion to conduct a search of the defendant's laptop. The reasoning of both the Fifth and Second Circuits would be consistent with a ruling that digital searches require reasonable suspicion, because both acknowledged that possibility and agents in both cases possessed the requisite reasonable suspicion. The Ninth Circuit's distinction between forensic searches and cursory searches in *Cotterman* is concerning because as technology advances, further clarification of these vague terms will be needed. Samuel A. Townsend, *Laptop Searches at the Border and United States v. Cotterman*, 94 B.U. L. Rev. 1745, 1768 (2014). Also, *Arnold* was decided in a pre-*Riley* world, and this Court specifically stated that a digital device's "immense storage capacity" *is* a relevant factor in evaluating if a search is reasonable. *Riley*, 134 S.Ct. at 2489. For all of these reasons, this Court can and should resolve this circuit split by requiring reasonable suspicion for digital devices at the border because of the increased risks to privacy inherent in such searches.

2. Although the search of Ms. Koehler's laptop occurred at the border, this Court's decision in *Riley* regarding the constitutionality of digital searches must be applied to the context of border searches.

The search of a laptop implicates all of the privacy-related concerns that the *Riley* court discussed in its analysis of a cell phone search, but with an even greater level of intrusion. See also Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005) (noting an 80-gigabyte hard drive is roughly equivalent to 40 million printed pages). In *Riley*, this Court held that because a cell phone search can reveal "the sum of an individual's private life," police officers must generally obtain a warrant before conducting such a search. *Riley*, 134 S.Ct. at 2485. In *Riley*, officers impounded the defendant's car after he was arrested for driving with a suspended license. *Id.* at 2480. An inventory search of the vehicle led officers to search through his cell phone, revealing evidence of his past crimes. *Id.* This Court clarified that the authority to conduct a search incident to arrest is based on concerns of officer safety and preservation of

evidence, but a cell phone does not pose a risk to officer safety in the same way a hidden weapon might, and a search of a cell phone does not prevent destruction of evidence. *Riley*, 134 S.Ct. at 2483 (citing *United States v. Robinson*, 414 U.S. 218 (1973)). Thus, this Court held that a cell phone search is not typically justified by a search incident to arrest. *Id.* at 2489.

While there are relatively few post-*Riley* decisions that speak to the border exception, a few district courts have attempted to grapple with this intersection of law. In *United States v. Kim*, F.Supp.3d 32, 40 (2015), the court held that the search of the defendant's laptop at the border was non-routine and lacked reasonable suspicion. *Id.* The court held that "evidence of prior criminal conduct alone is insufficient to give rise to reasonable suspicion of ongoing or imminent criminal activity" during a border stop, and defendant Kim's travel itinerary did not arouse suspicion beyond the agent's hunch that his laptop might contain incriminating evidence. *Id*. The *Kim* court also noted that while this Court did not specifically discuss the impact that *Riley* might have on searches of laptops at the border, it strongly implied that these searches cannot be fairly compared to searches of ordinary containers when evaluating privacy concerns. *Id.* at 54. The analysis of whether a search is reasonable under the Fourth Amendment "does not simply end with the invocation of . . . the well-recognized border exception, as broad as it may be." *Id.*

Ms. Koehler is entitled to protection from the unreasonable search of her laptop under this Court's decision in *Riley*. Both laptops and cell phones have the capacity to store emails and text messages, documents, contacts, and search engine histories, but a laptop has a greater storage capacity than a cell phone. This Court's holding in *Riley* suggests that storage capacity *is* a relevant factor that *does* speak to the reasonableness of a search. In reality, *any* digital search is inherently invasive, regardless of the quantity of documents opened. As the Thirteenth Circuit noted, "the fact that Agent Ludgate viewed already-opened documents has no bearing on the fact that [she]

had Ms. Koehler's entire world . . . at her fingertips." R. at 18. Furthermore, this Court has held that officers must generally obtain a warrant supported by probable cause before conducting a search of a cell phone incident to arrest. *Riley*, 134 S.Ct. at 2485. At the very least, border agents should be held to a reasonable suspicion standard before they conduct an invasive digital search on a device of a traveler who simply happens to be crossing the border. Importantly, Ms. Koehler was not even present during the border stop, and her past convictions and listing as a "person of interest" did not on their own indicate she was involved in crime. For these reasons, the search of Ms. Koehler's laptop violated the Fourth Amendment, and as such, this Court should hold that digital searches at the border require reasonable suspicion. Any other ruling would strip the Fourth Amendment of its legitimacy at the border in a digitally-dependent world.

II. THE USE OF INTRUSIVE SURVEILLANCE TECHNOLOGIES RESULTED IN VIOLATIONS OF MS. KOEHLER'S FOURTH AMENDMENT RIGHTS.

There is undeniable appeal in using cutting-edge technology to fight crime, but safety should not come at the cost of liberty. The warrantless use of drones and radars to intrude upon the liberty of the people cannot be tolerated. The Government intruded upon the sanctity of Ms. Koehler's home when it surveilled her with a PNR-1 drone and a Doppler radar, both of which constitute unreasonable searches in violation of her Fourth Amendment rights.

A. The Warrantless Deployment of the PNR-1 Drone Violated the Fourth Amendment Because Ms. Koehler Has a Reasonable Expectation of Privacy from Drone Surveillance.

The court of appeals is correct in holding that ECPD's warrantless use of the PNR-1 drone is an unreasonable search in violation of the Fourth Amendment. To determine if government surveillance is a "search" within the meaning of the Fourth Amendment, this Court uses the two-part *Katz* analysis. *Smith v. Maryland*, 442 U.S. 735, 739 (1979) (adopting *Katz*). The Fourth Amendment protects against government intrusion when "a person ha[s] exhibited an actual

(subjective) expectation of privacy" and that expectation is "one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). In *Katz*, electronically monitoring a phone call made within a telephone booth violated the privacy upon which a caller justifiably relies. *Id.* at 353 (majority opinion).

As a baseline, it is well established that private homes are constitutionally protected areas, whereas open fields are not. *Id.* at 351. n.8 (citing *Weeks v. United States*, 232 U.S. 383 (1914); *Hester v. United States*, 265 U.S. 57 (1924)). The Fourth Amendment also protects the area immediately surrounding a house, known as curtilage. *United States v. Dunn*, 480 U.S. 294, 300 (1987). In *Dunn*, a barn used to store and process noxious chemicals was outside the home's curtilage. *Id.* at 296-99. *Dunn* listed factors[1] that guide the curtilage analysis, but cautioned that combining factors will not yield a "correct" answer to curtilage questions. *Id.* at 301. Rather the *centrally relevant* consideration is "whether the area in question is so intimately tied to the home itself that it should be placed under the home's 'umbrella' of Fourth Amendment protection." *Id.*

The district court mischaracterized the pool area as not within the curtilage of Ms. Koehler's home. Mechanical reliance on the curtilage factors misses the heart of *Dunn*. The pool area is tied to the intimate activities of home and family life, and should be afforded full protections of the Fourth Amendment. Unlike the barn in *Dunn*, homeowners with pools frequently use their pool areas for intimate activities such as throwing parties, hosting family gatherings, exercising, and the like. Even if the pool area is not considered curtilage under *Dunn*, the curtilage doctrine is not a limit on Fourth Amendment protection. *Dow Chemical Co. v. United States*, 476 U.S. 227, 250 (1986) (Powell, J., concurring in part and dissenting in part). Overreliance on the *Dunn*

[1] *Dunn* lists four factors: (1) proximity of the area to the home; (2) whether the area is within an enclosure surrounding the home; (3) the nature of the uses for the area; and (4) steps taken to protect the area. *Dunn*, 480 U.S. at 301.

curtilage factors is misguided because the "Fourth Amendment protects people, not places." *Katz*, 389 U.S. 352.

Because the pool area is protected, the aerial surveillance performed on it poses a threat to Ms. Koehler's reasonable expectation of privacy. This Court has resolved several aerial surveillance cases using the *Katz* framework. The Fourth Amendment does not require police traveling in navigable airspace to obtain a warrant before making naked eye observations. *California v. Ciraolo*, 476 U.S. 207, 215 (1986). In *Ciraolo*, police received a tip that marijuana was growing in defendant Ciraolo's backyard. *Id.* at 209. Officers were unable to observe the yard from ground level because of surrounding fences. *Id.* Officers then flew a private plane over Ciraolo's house at an altitude of 1,000 feet, allowing them to identify marijuana plants growing in the yard. *Id.* Although Ciraolo manifested a subjective expectation of privacy by putting up a fence, this Court concluded that it was not objectively reasonable to expect protection from aerial observation. *Id.* at 211, 214. This Court reasoned that the observations were physically nonintrusive and took place within public navigable airspace, where any member of the public could have seen what the officers had observed. *Id.* at 213-14.

In *Dow Chemical*, this Court held that because the uncovered areas of a 2,000-acre industrial complex are less like the "curtilage" of a home and more like an "open field," the Government's aerial photography from navigable airspace was not a search. *Dow Chemical*, 476 U.S. at 239. This Court reasoned that there can be no reasonable expectation of privacy for "activities out of doors in fields, except in the area immediately surrounding the home." *Id.* at 235-36 (quoting *Oliver v. United States*, 466 U.S. 170 (1984)).

This Court again upheld the constitutionality of aerial surveillance when police flew a helicopter at 400 feet and observed marijuana inside a greenhouse behind a mobile home. *Florida*

v. Riley, 488 U.S. 445, 448 (1989). Like *Ciraolo*, defendant Riley had a subjective expectation that his greenhouse would not be open to public inspection. *Id.* at 448, 450. This Court, however, again concluded that there was no reasonable expectation of privacy where the helicopter was legally flying over the property, and that this would be a "different case if flying at that altitude had been contrary to law or regulation." *Id.* at 450-52.

To the first *Katz* prong, Ms. Koehler has exhibited her subjective desire for privacy. The first prong is not a high bar. A person who "occupies [a telephone booth], shuts the door behind him, and pays the toll" as Katz did is "surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. *Katz*, 389 U.S. at 352. Ms. Koehler is likewise entitled to assume that her activities within an abandoned property she purchased on the outskirts of town—where visibility is limited—will not "broadcast" her presence to the world, much less be under aerial surveillance. Ms. Koehler further manifested her subjective expectation of privacy by using her alias and shell company to purchase Macklin Manor. *See United States v. Broadhurst*, 805 F.2d 849 (9th Cir. 1986) (holding that use of false names in the purchase of property, inter alia, demonstrates a subjective expectation of privacy).

As to the second *Katz* prong, this Court's analysis of the objective reasonableness of an expectation of privacy from aerial surveillance considers whether the aircraft is operated in compliance with the law and whether the public travels with sufficient regularity through the airspace in question. *Florida v. Riley*, 488 U.S. at 451 n.3; *Id*. at 464-465 (Brennan, J., dissenting). The district court held that the use of the PNR-1 drone was valid because it was performed in a nonintrusive manner in navigable airspace where any member of the public could legally be. However, the assertion that ECPD operated the PNR-1 drone in navigable airspace and in compliance with the law is difficult to defend upon closer inspection of the governing Federal

Aviation Administration (FAA) regulations.[2] The PNR-1 has likely violated several FAA regulations,[3] which distinguishes its use from the permissible aerial observations in *Ciraolo*, *Dow Chemical*, and *Florida v. Riley*, where police complied with FAA regulations. ECPD's use of the PNR-1, however, is objectively unreasonable *even if* it did not break any laws. The proper inquiry is not whether a law enforcement aircraft complies with FAA regulations, but whether it is "in the public airways at an altitude at which members of the public traveled with sufficient regularity." *Florida v. Riley*, 488 U.S. at 454 (O'Connor, J., concurring).[4]

The aerial surveillance of Ms. Koehler's property intruded on her reasonable expectation of privacy not only because the drone violated FAA regulations, but also because members of the public do not fly with sufficient regularity near Macklin Manor. In fact, planes and other aircraft avoid the area due to the poor visibility caused by perpetual cloud and fog. Unlike *Riley* where the expectation of privacy is "rendered illusory by the extent of public observation," Ms. Koehler's

---

[2] FAA regulations are codified in Title 14 of the Code of Federal Regulations (CFR). eCFR – Code of Federal Regulations, https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title14/14tab_02.tpl (last visited October 20, 2017).

[3] The following are just a few examples of likely violations. First, the PNR-1 violated the prohibition against operation during civil twilight since Officer Lowe deployed it at dawn. 14 C.F.R. § 107.29. Second, Officer Lowe "lost track of [the PNR-1] for about 4-5 minutes" and "lost track of the drone's altitude." R. at 41. Her inability to determine the drone's altitude violates 14 C.F.R. § 107.31. Third, ECPD flew the drone over Ms. Koehler's person, in violation of the prohibition against flying a drone over other human beings. 14 C.F.R. § 107.39. Fourth, Officer Lowe knew that the PNR-1 had network connectivity errors that would affect her control of its altitude. R. at 41. This violated the requirement that the operator must "[e]nsure that all control links between [the] ground control station and the small unmanned aircraft are working properly." 14 C.F.R. § 107.49. Finally, visibility around Macklin Manor was poor and there were a lot of clouds when Officer Lowe deployed the PNR-1. R. at 41. This likely violated drone operation limits regarding visibility and distance from clouds. 14 C.F.R. § 107.51(c) & (d).

[4] A five-justice majority—including Justice Blackmun in his dissent, and Justices Marshall and Stevens joining in Justice Brennan's dissent—agree that Justice O'Connor, rather than the plurality in *Riley*, asks the proper inquiry for assessing the objective reasonableness of an expectation of privacy from aerial surveillance.

expectation of privacy on a secluded mountaintop, free from regular air traffic, is one that society is prepared to recognize as reasonable. *Florida v. Riley*, 488 U.S. at 464-465 (Brennan, J., dissenting). The operation of the PNR-1 drone in this rarely used airspace is thus an unreasonable search in violation of Ms. Koehler's Fourth Amendment rights.

B. The Warrantless Use of the Doppler Radar to Scan Ms. Koehler's Home Violated the Fourth Amendment Because It Revealed Information that Would Not Otherwise Be Obtainable Without Entering the Home and Because Such Devices Are Not in General Public Use.

The court of appeals is also correct in holding that the police's warrantless use of the Doppler radar is an unreasonable search in violation of Ms. Koehler's Fourth Amendment rights, and that the radar is completely analogous to the thermal imaging device used in *Kyllo v. United States*, 533 U.S. 27 (2001). There, the Government used a thermal imager—which detects infrared radiation not visible to the naked eye—to scan defendant Kyllo's home from the streets in front of and behind his property. *Id.* at 29-30. The scan revealed hot spots in Kyllo's home, consistent with the Government's suspicion that he was using high-intensity lamps to grow marijuana inside. *Id.* at 30. This Court held that the Government's use of a device that is not in general public use, to explore details of a home that would previously have been unknowable without physical intrusion, constitutes a search subject to the Fourth Amendment. *Id.* at 40.

The district court comes to incorrect conclusions for both prongs of *Kyllo*. First, the information gained about Ms. Koehler's home could not have otherwise have been obtained without physical intrusion. Second, Doppler radars are not in general public use.

1. The information that the Doppler radar device gained would not have otherwise been obtainable without entering Ms. Koehler's home.

For the first prong, the court of appeals correctly held that the information gained about the inside of Ms. Koehler's home and pool house could not have been obtained without the Doppler

radar. The district court's contrary conclusion that the information obtained by the radar was merely that people were present inside the house and pool house is patently untrue. Crucially, the Doppler radar revealed the number of people inside and their general location and movements, which undoubtedly led the officers to conclude that the Ford children were being held hostage in the pool house. The scan of the pool house revealed three individuals, close together, breathing but unmoving, which likely lead to the inference that these were the three Ford children. The scan also revealed that another person appeared to be pacing around near the three unmoving individuals, leading to the presumption that this fourth person was standing guard. These details would previously have been unknowable without physical intrusion into Ms. Koehler's home and pool house. That the officers made additional inferences based on the scans to reach their conclusion does not insulate the unlawful search. *Kyllo*, 533 U.S. at 36-37.

The possibility that information equivalent to that obtained by the radar could have been obtained by other means does not excuse the Fourth Amendment violation. *Id.* at 35 n.2. For example, police can lawfully set up year-round visual surveillance outside of a home to determine how many people are inside, "but that does not make breaking and entering to find out the same information lawful." *Id.* The use of the Doppler radar is unlawful, and the proposition that officers *may* have found out who was inside using some other means is irrelevant. The district court merely speculated that Officer Hoffman would have eventually seen the people inside Macklin Manor walk outside.[5] R. at 11. Notwithstanding the slim chance that Officer Hoffman would have seen *all* the occupants of the two buildings in one morning, the use of the radar is not made lawful because it obtained intimate details regarding the number, location, and movements of individuals

[5] Unlike the year-round surveillance hypothetical, Officer Hoffman was conducting foot surveillance for less than four hours. ECPD arrived at 4:30 a.m., left at one point, and returned at 8:00 a.m. the same morning with search warrant in hand. R. at 4-5.

within a building. When it comes to the home, this Court has emphasized that "*all* details are intimate details" regardless of the level of intrusion because "the entire area is held safe from prying government eyes." *Kyllo*, 533 U.S. at 37.

2. Doppler radar devices are not in general public use.

The district court held that Doppler radar devices are in "common use" because they have become extremely popular among law enforcement, but popularity of a technology within the law enforcement community is not the test. R. at 11. Rather, the second prong of *Kyllo* asks if a technology is in "general *public* use" as the court of appeals correctly recognized. *Kyllo*, 533 U.S. at 34 (emphasis added). *Kyllo* illustrated the meaning of "general public use" by drawing a comparison to the air travel at issue in *Ciraolo*. *Id.* at 40 n.6. While "private and commercial flight in the public airways is routine" and it was unreasonable for Ciraolo to expect protection from naked eye observation of his property, the use of thermal imaging technology on a private home is *not* routine. *Id.* Thus, whether a technology is in general public use is linked to how routinely it occurs or is used outside of law enforcement.

Doppler radar is less like commercial air travel and is more like thermal imaging in that its use is not routine by any stretch of the imagination. Devices like that used on Ms. Koehler's home are even less available to the public than the thermal imagers employed in *Kyllo* and are therefore even less routinely used.[6] Detective Perkins' testimony is damning for this prong. When asked whether Doppler radars are available on websites such as Amazon, Perkins responded "[n]ot that

[6] For example, FLIR Systems, Inc., a leader in thermal imaging infrared cameras, markets and sells a variety of thermal imaging products to the public, many at a price point of just a few hundred dollars. Flir Systems | Thermal Imaging, Night Vision and Infrared Camera Systems, http://www.flir.com (last visited October 20, 2017). Indeed, FLIR products are even available on Amazon. Amazon.com: flir, https://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3 Daps&field-keywords=flir com (last visited October 20, 2017).

I'm aware. The Department special orders them directly from the manufacturer." R. at 35. When asked whether "the radar devices [are] popular amongst the public," Perkins responded that he doesn't believe so. R. at 35. Detective Perkins further explains how Doppler radars "really are built for law enforcement purposes," that he "[doesn't] see any reason why the average citizen would own one," and that he doesn't think that he has ever seen a civilian use one. R. at 35. Because Doppler radar has no apparent use beyond law enforcement and because such devices are difficult for the average consumer to even obtain, it is not in "general public use."

3. The Scan of Ms. Koehler's home with the Doppler radar violated her reasonable expectation of privacy and was thus a search within the meaning of the Fourth Amendment.

As the district court pointed out, *United States v. Denson*, 775 F.3d 1214 (10th Cir. 2014) is the first case that directly addresses Doppler radars. Justice Gorsuch, then serving as a Circuit Judge for the Tenth Circuit, expressed concern about the potentially problematic nature of radar searches. *Id.* at 1218. The opinion warned that warrantless use of Doppler radars poses grave Fourth Amendment questions and that such technology creates the "risk for abuse and new ways to invade constitutional rights." *Id.* Although *Denson* declined to rule on the constitutionality of warrantless Doppler radar scans, this Court can definitively do so here. *Id.* at 1218-19.

A Doppler radar is even more intrusive than the thermal imager used in *Kyllo*. A thermal imager "[does] not show any people or activity within the walls of the structure[,] . . . cannot penetrate walls or windows to reveal conversations or human activities[,]" and only shows "amorphous 'hot spots . . .'" *Kyllo*, 533 U.S. at 30-31. A Doppler radar shows much more. It zeroes, or "keys in" on people breathing, and reveals people and their activity behind walls. R. at 4, 33. Moreover, unlike the agents in *Kyllo* who performed the thermal scan from the street, Detective Perkins needed to surreptitiously approach the front of the main house in order to use

the radar. R. at 4. The area immediately surrounding the house is unquestionably within the curtilage and enjoys protection from police activity. *Florida v. Jardines*, 569 U.S. 1, 6 (2013).

Finally, this Court cautioned in *Kyllo* that the two-pronged rule it adopted "must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36. This Court contemplated developing technologies that sound strikingly similar to the Doppler radar, such as a "'Radar Flashlight' that 'will enable law officers to detect individuals through interior building walls.'" *Id.* at 36 n.3. The intrusiveness of powerful technologies like Doppler radar is exactly what the Court had in mind as it considered the impact of *Kyllo* on future technologies. The warrantless use of the Doppler radar—a device exclusively used by law enforcement—to reveal activities within the home intruded upon Ms. Koehler's reasonable expectation of privacy and thus violated her Fourth Amendment rights.

C. There Was No Probable Cause to Support a Search Warrant Absent the Illegal Border Search, Drone Search, and Doppler Radar Search, and the Resulting Fruits of the Poisonous Tree Must Be Suppressed.

The issue of "poisonous fruit" is not presented on certiorari. Nevertheless, because the district court comes to a different conclusion than the court of appeals as to whether there was probable cause to support a search warrant absent the drone and radar search, it is important to reiterate the persuasive reasoning of the Thirteenth Circuit. A search warrant requires probable cause, where under the totality of the circumstances, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 232, 238 (1983). Under the totality of the circumstances, Mr. Wyatt's $10,000 in cash cannot be linked to the kidnapping. The money was coming *into* the country, and it defies logic and practicality that a kidnapper would request money to be sent out of the country first, only to face inspection when returning through the U.S. border. That Mr. Wyatt is associated with Ms. Koehler, one of a

potential multitude of persons of interest, does not turn Ms. Koehler into the sole suspect. The additional evidence obtained from Ms. Koehler's laptop with documents relating to Mr. Ford and Macklin Manor cannot be used to support the search warrant because they are illegal searches whose fruits must be suppressed. Without the illegal drone and radar searches which confirmed Ms. Koehler's presence at Macklin Manor and led to the inference that the three Ford children were being held in the pool house, there is nothing under the totality of the circumstances to link Macklin Manor to the kidnapping. The search warrant for Macklin Manor obtained by ECPD was tainted by the prior illegal searches, and the subsequent, violent SWAT raid of Ms. Koehler's home without a valid warrant supported by probable case is presumptively unreasonable.

CONCLUSION

This Court should affirm the lower court's ruling on the border search issue. The simple fact that a traveler is at the border does not mean that all Fourth Amendment protection is lost. The border agents failed to establish the requisite reasonable suspicion to conduct a non-routine search of Ms. Koehler's laptop, and thus the search was unreasonable. Furthermore, this Court's ruling in *Riley* should be extended to border searches because of the increased threat to privacy involved in searching digital devices such as Ms. Koehler's laptop. This Court should also affirm the lower court's ruling on the drone and radar issue. The PNR-1 violated several FAA regulations, and Ms. Koehler's objective expectation of privacy is reasonable because there is no regular air travel near Macklin Manor. Furthermore, the Doppler radar is not in general public use, and it revealed intimate details of the home. Use of these intrusive technologies constitute illegal searches, and no probable cause exists without their observations. For the foregoing reasons, this Court should affirm the ruling of the Court of Appeals for the Thirteenth Circuit.