Docket NO. 04-422

IN THE

Supreme Court of the United States

Fall 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

RESPONDENT'S BRIEF ON THE MERITS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

STATEMENT OF THE ISSUES

1. Under federal law, is a warrantless search of a laptop at a border station valid under the border search exception when digital devices, including a searched laptop, carry a heightened privacy interest beyond the permissible scope of the exception, the border agents do not rely on the searched party's criminal history to justify increased suspicion, the laptop does not belong to the searched party, and the searched party's failure to declare over $10,000 does not relate to the contents or use of the laptop?

2. Under federal law, does police use of a PNR-1 drone and handheld Doppler radar constitute an impermissible search of a home when the PNR-1 drone surveys an area that falls within the home's remote, naturally-enclosed curtilage that is not visible from a public, routinely-used airspace, the Doppler radar exclusively used by police officers detects the number of people and their positioning in the home, and the evidence obtained from a prior border search of the homeowner's fiancé, allegedly relied on to obtain a search warrant for the home, does not show how the home related to the homeowner's suspected crime?

STATEMENT OF THE FACTS

I. Factual Overview

This case involves the U.S. Border Patrol's warrantless search of Ms. Koehler's laptop at the Eagle City border station. It further involves the impermissible searches of Macklin Manor carried out by a PNR-1 drone and handheld Doppler radar device.

The Border Stop. On August 17, 2016, U.S. Border Patrol Agents Dwyer and Ludgate stopped Scott Wyatt at the Eagle City border station. R. at 2. Despite appearing nervous and uncomfortable, Mr. Wyatt fully complied with the agents' request to conduct a routine border search of his vehicle. *Id.* When Agent Dwyer asked Mr. Wyatt to open his trunk, he found $10,000 in $20 bills and a laptop inscribed with the initials "AK." *Id.* Upon further questioning, Mr. Wyatt stated he shared the laptop with his fiancé, Ms. Amanda Koehler. *Id.*

The Warrantless Laptop Search. The agents next ran Ms. Koehler's name in their criminal database, but did not appear to check whether Mr. Wyatt had a criminal history. *See id.* They discovered Ms. Koehler had several previous criminal convictions for violence and was a person of interest in the recent kidnappings of the Ford children. *Id.* Agent Ludgate then opened Ms. Koehler's laptop and began searching its contents without Mr. Wyatt's consent and without a search warrant. R. at 2, 27–28. Agent Ludgate did not merely open the laptop and shut it—she opened it and meticulously read several open documents. R. at 3. Some documents contained the personal information of Timothy H. Ford—the missing children's father. *Id.* Agent Ludgate next found a lease agreement with an address that bore the name "Laura Pope." *Id.* The lease agreement information traced to Macklin Manor, an estate owned by "Laura Pope," an alias of Ms. Koehler. *Id.* Only then did she place Mr. Wyatt under arrest for failure to declare in excess of $10,000 in violation of 31 U.S.C. § 5136—a crime entirely unrelated to the contents of Ms. Koehler's laptop.

Id. Agent Ludgate provided the Eagle City Police Department with the evidence, and Detective Perkins, along with Officers Lowe and Hoffman, set out to conduct surveillance on the estate. *Id.*

The Macklin Manor Search. Macklin Manor lies on the outskirts of Eagle City atop Mount Partridge, a mountain covered year-round by fog and clouds. *Id.* Due to poor visibility, aircrafts typically avoid the mountain airspace. R. at 3, 42. The estate lacks a fence or gate. R. at 4.

Officer Lowe utilized a PNR-1 drone—equipped with a high-definition camera—to hover over the estate to obtain images of the main house, pool house, and pool area where Ms. Koehler was seen walking toward the pool house. R. at 4, 39. The PNR-1 drone usually flies at the legal maximum altitude of 1,640 feet, but during the estate surveillance it possibly exceeded this height due to network errors and flew as high as 2,000 feet. *See* R. at 4, 41. The drone hovered over the estate for 15 minutes, a duration necessary because of low visibility. *Id.*

Next, Detective Perkins used a Doppler Radar, without a warrant, to scan the front door area of the main house and the outside of the pool house. R. at 4. This device emits radio waves into buildings to detect movements or breathing up to fifty feet, thus establishing the number of people within a home, along with their relative location and disposition. R. at 4, 33. It is popular amongst law enforcement, but not manufactured or marketed to the public. R. at 35. The main house scan showed one person near the front door, and the pool house scan showed three individuals, close together and unmoving, and another presumably standing guard. R. at 5.

Detective Perkins felt that the border search established probable cause to search Macklin Manor, so after conducting the PNR-1 drone and Doppler radar surveillance, the ECPD obtained a search warrant. R. at 5, 34. Following forcible entry, Officers Lowe and Hoffman identified and captured Ms. Koehler. *Id.* The ECPD found the three Ford children, along with an individual standing guard, in the pool house. *Id.*

II. Procedural History

Ms. Koehler Moves to Suppress Evidence. The District Court denied Ms. Koehler's Motion to Suppress, holding the government's warrantless search of Ms. Koehler's laptop at the Eagle City border station was constitutional because the border search exception extends to the contents of a laptop. R. at 6, 13. The District Court also deemed permissible the warrantless searches of Macklin Manor conducted by the PNR-1 drone and the Doppler radar device. *Id.* Additionally, it found that Ms. Koehler failed to show impermissible "fruits" resulting from these searches because the detectives established probable cause from the border search evidence prior to using the PNR-1 drone and Doppler radar. R. at 11, 13.

Ms. Koehler Appeals Motion to Suppress. The Court of Appeals for the Thirteenth Circuit reversed the District Court's denial of the Motion to Suppress and remanded for further proceedings. R. at 21. The Thirteenth Circuit held digital border searches fall outside the scope of the border search exception, and in the alternative, Ms. Koehler's laptop search was non-routine and unsupported by reasonable suspicion. R. at 15. Additionally, it held the officers' warrantless use of the PNR-1 drone and Doppler radar device violated Ms. Koehler's Fourth Amendment rights. R. at 18. It further found the officers lacked probable cause for a search warrant without the information obtained from these devices; thus any evidence the officers gathered were "fruits" from the search that must be suppressed. R. at 21.

The Court Grants Petition for Certiorari. The Court granted certiorari to determine whether the government's warrantless border search of Ms. Koehler's laptop was a permissible search pursuant to the border search exception. R. at 22. In addition, the Court will address whether the officers' warrantless use of a PNR-1 drone and handheld Doppler radar device violated Ms. Koehler's Fourth Amendment rights. *Id.*

SUMMARY OF THE ARGUMENT

I. Unconstitutional Laptop Border Search

Border searches are narrow exceptions to the Fourth Amendment's warrant requirement. While the government may conduct discretionary routine border searches, non-routine searches require a showing of reasonable suspicion prior to search. A routine search generally includes searching a person's vehicle or luggage. By contrast, non-routine searches are those particularly offensive as to justify increased suspicion, such as an intrusive search of a person or, as Respondent argues in this case, a digital border search.

In this case, Agent Ludgate's border search of Ms. Koehler's laptop was wholly unconstitutional. Under this Court's logic in *Riley v. California*, digital devices should be free from warrantless searches altogether because the immense storage capacity of a digital device heightens a person's reasonable expectation of privacy. But if this Court finds digital devices are subject to the border search exception, such searches are undoubtedly non-routine. Here, Agent Ludgate did not have reasonable suspicion to search Ms. Koehler's laptop because Mr. Wyatt was the border crosser—not Ms. Koehler. Further, the agents did not rely on information of any prior convictions for Mr. Wyatt or Ms. Koehler relating to the inherent use of a laptop. The government thus fails to prove reasonable suspicion to search Ms. Koehler's laptop. Therefore, this Court should suppress all evidence stemming from the unconstitutional Eagle City border station search.

II. Impermissible Drone and Doppler Radar Searches

Warrantless searches of a home or curtilage are impermissible without a showing that the homeowner lacks a reasonable expectation of privacy over the searched premises. Specifically, aerial searches of a person's curtilage cannot occur when an individual has a subjective expectation of privacy over their curtilage that society deems reasonable, and when the curtilage is not susceptible to naked-eye observation from a publicly-accessible airspace. Here, the PNR-1 drone

surveillance of the property constituted an impermissible search because the pool house and pool area fall within Macklin Manor's remote curtilage. Further, the estate avoids aerial observation due to the lack of proximate and routine use of the airspace and the inability for naked-eye observation resulting from perennial fog and cloud cover.

The use of a handheld Doppler radar on someone's home and curtilage cannot occur without showing the resulting information is otherwise obtainable without physical intrusion and that the technology is generally in common use. Here, the use of the Doppler radar to scan the main home and pool house was an impermissible search because the information gathered—the location and disposition of individuals within the estate—was unobtainable without being physically within the home. Further, the Doppler radar does not enjoy common use because it is unavailable for public purchase and is exclusively deployed by police officers.

The Court must suppress evidence resulting from the impermissible searches notwithstanding a showing that probable cause existed prior to the searches. Probable cause requires that, in the totality of the circumstances, an objective police officer could draw a connection between a specific location and the finding of evidence of a crime. Here, the border search evidence did not meet this requirement—the $10,000 in 20s, the Ford Family information, and the deed records did not establish the relationship between the estate and the crime. Therefore, this Court should suppress all impermissible fruits of the PNR-1 drone and Doppler radar searches.

STANDARD OF REVIEW

Appellate courts apply a bifurcated standard of review to a district court's denial of a motion to suppress. *United States v. Belton*, 520 F.3d 80, 82 (1st Cir. 2008). This standard reviews the district court's findings of fact for clear error and conclusions of law—including Fourth Amendment issues—de novo. *See id.*

ARGUMENT

The Court of Appeals for the Thirteenth Circuit properly reversed the District Court's denial of the Motion to Suppress because the warrantless search of Ms. Koehler's laptop at the Eagle City border station exceeded the scope of the border search exception, and because the use of the PNR-1 drone and Doppler radar on Macklin Manor constituted invasive searches in violation of Ms. Koehler's reasonable expectation of privacy. The Fourth Amendment seeks to protect "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches . . . ." U.S. Const. amend. IV. Warrant and probable cause requirements enforce and solidify these protections, with exceptions permitted in very narrow, specifically-established circumstances. *See Katz v. United States*, 389 U.S. 347, 357 (1957).

I. THE LAPTOP SEARCH WAS UNCONSTITUTIONAL BECAUSE IT EXCEEDED THE SCOPE OF THE BORDER SEARCH EXCEPTION.

The Thirteenth Circuit properly ruled that digital devices fall outside the scope of the border search exception, rendering the U.S. Border Patrol search of Ms. Koehler's laptop unconstitutional. Border searches operate within a narrow exception to the Fourth Amendment's warrant requirement, which provides that routine border searches do not require reasonable suspicion, probable cause, or a warrant. *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985); *see United States v. Seljan*, 547 F.3d 993, 999 (9th Cir. 2008). Courts, however, recognize that border searches "carry grave potential for arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals." *Montoya de Hernandez*, 473 U.S. at 556 (internal quotations omitted). Thus, courts limit border searches by balancing individual privacy rights against government interests. *See United States v. Cotterman*, 709 F.3d 952, 960 (9th Cir. 2013).

In this case, Agent Ludgate's warrantless search of Ms. Koehler's laptop is unconstitutional because digital devices fall outside the narrow scope of the border search exception. Even if laptops lie within reach, the U.S. Border Patrol still violated Ms. Koehler's Fourth Amendment rights because Agent Ludgate lacked the necessary reasonable suspicion to conduct a non-routine digital search.

A. The Warrantless Search was Unconstitutional Because in the Wake of *Riley*, the Border Search Exception Does Not Apply to Digital Devices.

The warrantless border search of Ms. Koehler's laptop was unconstitutional because Agent Ludgate unreasonably believed the border search exception extends to digital devices. Whether warrantless searches of digital devices may be conducted at the border falls squarely within the Supreme Court's recent decision in *Riley v. California*, 134 S. Ct. 2473, 2491 (2014). In its unanimous opinion, the Court held officers must generally secure a warrant before conducting a data search on cell phones. *Id.* at 2493. While upholding the "search incident to arrest" warrant exception to the Fourth Amendment, the Court held cell phone data searches do not apply absent "exigent circumstances."[1] *Id.* Many cell phones are like "minicomputers" containing the "privacies of life" that far outweigh privacy concerns implicated by the search of a wallet or purse. *Id.* at 2488–89, 94–95. As a result, cell phone technology involves the "very sensitive privacy interests that this Court is poorly positioned to understand and evaluate." *Id.* at 2497.

Circuit courts upholding digital border searches are erroneous in the wake of *Riley*. Prior to *Riley*, courts analogized a laptop to a mere closed container subject to complete search at the

1. The border search exception is not based on "exigent circumstances." *United States v. Ramsey*, 431 U.S. 606, 621 (1977) ("[T]he border search exception . . . is a[n] exception to the Fourth Amendment's general principle that a warrant be obtained, and in this respect is like the similar search incident to lawful arrest exception. . . .") (internal quotations omitted).

border. *See, e.g.*, *United States v. Arnold*, 533 F.3d 1003, 1007 (9th Cir. 2008); *United States v. Ickes*, 393 F.3d 501, 504 (4th Cir. 2005). In *Arnold*, the Ninth Circuit alarmingly held customs officials do not need reasonable suspicion to search a laptop at the border. 533 F.3d at 1009. The court reasoned, "[c]ourts have long held that searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment." *Id.* at 1007; *see also Ickes*, 393 F.3d at 504 (holding a traveler's computer and disks were searchable "goods" synonymous to "cargo" within the meaning of the relevant statute). Yet this analysis directly conflicts with the Court's holding in *Riley*—laptop computers, like cell phones, are fundamentally distinct from traditional closed containers. *See* 134 S. Ct. at 2491 ("[T]he analogy [of equating a cell phone to a container] crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen.").

Since *Riley*, no circuit court has addressed the validity of the border search exception in the electronic data context. Many legal scholars are struggling with digital border searches in light of *Riley's* extreme deference to electronic privacy. *See* Eunice Park, *The Elephant in the Room: What Is A "Nonroutine" Border Search, Anyway? Digital Device Searches Post-Riley*, 44 Hastings Const. L.Q. 277, 312 (2017); Thomas Mann Miller, *Digital Border Searches After Riley v. California*, 90 Wash. L. Rev. 1943, 1995 (2015). One scholar agrees *Riley* may eliminate digital devices from the border search exception entirely. *See* Miller, *supra*, at 1995.

Very few district courts have entertained electronic border searches post-*Riley*. At least one court held a laptop border search was so invasive of a traveler's privacy that it violated his Fourth Amendment rights. *See United States v. Kim*, 103 F. Supp. 3d 32, 56–57 (D.D.C. 2015). Other courts impliedly view digital border searches as "non-routine," valid only with support from particularized, reasonable suspicion. *See, e.g.*, *United States v. Wanjiku*, No. 16 CR 296, 2017 WL

1304087, at *5 (N.D. Ill. Apr. 7, 2017) (declining to label a laptop border search as routine or non-routine but finding reasonable suspicion to search the laptop for child pornography); *United States v. Furukawa*, No. CRIM 06-145 DSD/AJB, 2006 WL 3330726, at *1 (D. Minn. Nov. 16, 2006) ("[T]he court need not determine whether a border search of a laptop is "routine" for purposes of the Fourth Amendment because . . . the customs official had a reasonable suspicion in this case.").

The present case illustrates the need for this Court to hold that border searches of laptops must comply with the Fourth Amendment warrant requirement, thereby falling outside the scope of the border search exception. Here, Agent Ludgate violated Ms. Koehler's Fourth Amendment rights when she opened Ms. Koehler's laptop and searched its contents at the Eagle City border station. *See* R. at 2–3. Laptop computers carry equal—if not higher—privacy implications than the cell phone data at issue in *Riley*. *See* 134 S. Ct. at 2488–89. Further, the case at bar distinguishes from the "container" line of cases, as *Riley* recognized the uniquely sensitive nature of digital data compared to a mere physical object. *See id.* at 2491. *Cf. Arnold*, 533 F.3d at 1007; *Ickes*, 393 F.3d at 504. Even if this Court is unpersuaded to remove digital devices from the border search exception, it may follow the "non-routine" line of cases that justify searches only where reasonable, individualized suspicion is present. *See Wanjiku*, 2017 WL 1304087, at *5; *Furukawa*, 2006 WL 3330726, at *1.

Expanding the border search exception to include digital data would be like searching an individual's home without a warrant—the gravest Fourth Amendment abuse possible. *See Riley*, 134 S. Ct. at 2491 ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house."). Under this standard, Agent Ludgate's warrantless border laptop search violated Ms. Koehler's Fourth Amendment rights. Consequently, the Thirteenth Circuit properly reversed the lower court's denial of the Motion to Suppress.

B. Even if the Border Search Exception Applies, the Present Search is Unconstitutional Because it was Non-routine and Lacked Reasonable Suspicion.

Assuming, *arguendo*, that the border search exception may permit warrantless digital border searches in limited circumstances, Agent Ludgate's laptop search is wholly unconstitutional because she lacked any reasonable suspicion to search its contents. Border searches avoid strict Fourth Amendment mandates when those searches are routine. *See Montoya de Hernandez*, 473 U.S. at 538. *Non-routine* border searches, however, must be justified by a border agent's reasonable, particularized suspicion of wrongdoing. *Id.* at 541. Whether a particular search is non-routine is a case-specific question of fact. *Id.*

Routine border searches generally involve the search of an individual's vehicle or luggage. *See United States v. Flores-Montano*, 541 U.S. 149, 156 (2004) (holding the border agents' removal, disassembly, and reassembly of an entrant's vehicle fuel tank is routine); *see also United States v. Ezeiruaku*, 936 F.2d 136, 143 (3d Cir. 1991) (holding the border search of a traveler's luggage is routine). By contrast, non-routine border searches are more invasive and generally involve an intrusive search of a person, such as a body cavity search. *See Montoya de Hernandez*, 473 U.S. at 541. While the lines between routine and non-routine searches remain blurred, the Court leaves open the additional question of when a "particularly offensive" search might fail the reasonableness test. *Id.* at 155 n.2 (citing *United States v. Ramsey*, 431 U.S. 606, 618 n.13 (1977)).

1. *Laptop border searches are non-routine and comparable to the intrusive border search of a person.*

Agent Ludgate's border search of Ms. Koehler's laptop was non-routine because the immense storage capacity of a digital device entirely changes a person's reasonable expectation of privacy. *See Riley*, 134 S. Ct. at 2489. The Court has not provided a definition for the outer limits of a non-routine search. *See Flores-Montano*, 541 U.S. at 156. Instead, the level of intrusion on a person's privacy more easily distinguishes non-routine searches from routine searches. *See United*

States v. Irving, 452 F.3d 110, 123–24 (2d Cir. 2006). Therefore, if digital devices are within reach of the border search exception, such searches are undoubtedly non-routine.

Courts that uphold digital border searches often explicitly or impliedly categorize them as non-routine through the reasonable suspicion analysis. *See id.* at 124; *United States v. Roberts*, 274 F.3d 1007, 1014–15 (5th Cir. 2001). In *Roberts*, the court held the search of a traveler's computer diskettes was non-routine and supported by reasonable suspicion. 274 F.3d at 1014–15. Referencing the intricate balance of individual and government border interests, the court "[brought] into play only the most narrow constitutional basis" that "a non-routine outbound search is permissible when . . . (1) the outbound search is at the border or its functional equivalent; (2) Customs Agents have reasonable suspicion . . . and (3) the search is relatively unintrusive . . . ." *Id. Cf. Irving*, 452 F.3d at 124 (upholding the border search of a traveler's computer diskettes in light of reasonable suspicion, but declining to determine whether it was routine or non-routine).

Some courts, notably the Fourth and Ninth Circuits, egregiously view digital searches as routine. *See Cotterman*, 709 F.3d at 967; *Ickes*, 393 F.3d at 505. These courts fathom "manual" digital border searches to be less invasive than "forensic" examinations. *See Cotterman*, 709 F.3d at 967; *see also United States v. Saboonchi*, 990 F. Supp. 2d 536, 569 (D. Md. 2014) (deeming a forensic search of digital data non-routine but supported by reasonable suspicion). In *Cotterman*, the Ninth Circuit held the forensic examination of a border crosser's computer required reasonable suspicion, but quick manual searches did not. 709 F.3d at 967. This flawed reasoning sows confusion because any distinction between "manual" and "forensic" data searches thwarts the very privacy concerns *Riley* recognized. *See United States v. Ramos*, 190 F. Supp. 3d 992, 1002–03 (S.D. Cal. 2016) ("[A] manual search can be just as invasive as a full forensic examination,

rendering the two standards set forth by *Cotterman* both inconsistent with *Riley's* logic and impractical.").

The present case follows the non-routine line of digital border search cases. *See Irving*, 452 F.3d at 124; *Roberts*, 274 F.3d at 1012. Unlike the Fourth and Ninth Circuit's dismissal of digital searches as routine, laptops provide a "unique situation" because of their "boundless amount[s] of information." R. at 17; *see Cotterman*, 709 F.3d at 967; *Ickes*, 393 F.3d at 505. While Agent Ludgate's search of Mr. Wyatt's vehicle may have been routine, the laptop search was certainly not. R. at 27–28; *see Flores-Montano*, 541 U.S. at 156; *Montoya de Hernandez*, 473 U.S. at 541. Rather, a laptop search is more akin to an intrusive search because its capacity to store vast amounts of personal data heightens one's reasonable expectation of privacy. *See Riley*, 134 S. Ct. at 2489.

If this Court determines that electronic data falls within the grasp of the border search exception, it should categorize searches of laptops and similar devices as non-routine. To hold otherwise would undermine this Court's mandate in *Riley*. *See id*. Furthermore, non-routine searches require reasonable suspicion—here, Agent Ludgate lacked reasonable suspicion to search Ms. Koehler's laptop. Therefore, the search violated Ms. Koehler's Fourth Amendment rights, and the Thirteenth Circuit properly suppressed the evidence seized from her laptop.

2. *Non-routine border searches are unconstitutional absent particularized, reasonable suspicion.*

Agent Ludgate's non-routine search of Ms. Koehler's laptop was unconstitutional because the agents did not rely on Mr. Wyatt's criminal history, if any, to justify increased suspicion, and Mr. Wyatt's failure to declare over $10,000 was completely unrelated to Ms. Koehler's laptop. The Court defines reasonable suspicion as "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). The standard is satisfied when officers can point to "specific and articulable facts," that,

when considered with rational inferences drawn from those facts, indicate criminal activity "may be afoot." *Terry v. Ohio,* 392 U.S. 1, 21 (1968). Overall, a border agent's finding of reasonable suspicion must occur in light of the totality of the circumstances. *Cortez,* 449 U.S. at 417. In the absence of a clear test for reasonable suspicion, the Second Circuit provides a set of factors to consider, including the suspect's unusual conduct, the discovery of incriminating matter during routine searches, computerized information showing propensity to commit relevant crimes, or a suspicious itinerary. *Irving*, 452 F.3d at 124.

Courts only find reasonable suspicion to conduct a laptop border search where the traveler has a prior criminal history, particularly in the limited context of crimes inherently involving the use of digital devices. *See Irving*, 452 F.3d at 124; *Ickes*, 393 F.3d at 507; *United States v. Romm,* 455 F.3d 990, 994 (9th Cir. 2006). In *Irving*, the border entrant was a previously convicted pedophile who was subject to an ongoing criminal investigation into similar charges, and he stated he had visited an orphanage in Mexico. 452 F.3d at 124. All these facts, combined with additional evidence of children's books and drawings in his luggage, supported a finding of reasonable suspicion. *Id.* Likewise, in *Ickes*, the court deemed constitutional the agents' border search of a traveler's computer and disks because the agents did not inspect the computer until after discovering marijuana paraphernalia, photo albums of child pornography, a disturbing video focused on a young ball boy, and an outstanding warrant for the suspect's arrest. 393 F.3d at 507; *see also Romm,* 455 F.3d at 994 (finding constitutional the warrantless search of a traveler's computer where he had prior convictions of child pornography and was currently on probation).

Importantly, the existence of a prior criminal record does not per se guarantee the presence of reasonable suspicion. For instance, even where one traveler had a prior criminal record, one court still held there was no reasonable suspicion to conduct a laptop search at the border. *See Kim,*

103 F. Supp. 3d at 56–57. Unlike the line of cases involving child pornography offenses, this case involved a traveler's prior violation of export laws. *Id.* The court held that because the traveler's previous incident did not involve travel to the United States, and border agents did not conduct surveillance on the traveler while he was in the country, there was no reasonable suspicion to search his laptop. *Id.*

In the present case, Agent Ludgate lacked reasonable suspicion to search Ms. Koehler's laptop. Unlike the line of cases involving child pornography, the border agents did not suspect Mr. Wyatt of a crime inherently involving the use of a laptop. *See* R. at 2–3; *Ickes*, 393 F.3d at 507. Rather, Mr. Wyatt failed to declare an excess of $10,000—a crime akin to the export control violation seen in *Kim*. R. at 3; *see Kim*, 103 F. Supp. 3d at 56–57. In addition, the reasonable suspicion analysis hinges on whether the *border crosser*, Mr. Wyatt, has a criminal history—not Ms. Koehler. *See Irving*, 452 F.3d at 124; *Romm*, 455 F.3d at 994; *Ickes*, 393 F.3d at 507. Here, the record does not indicate the border agents searched Mr. Wyatt's criminal history for past convictions. *See* R. at 2; *Irving*, 452 F.3d at 124; *Romm*, 455 F.3d at 994; *Ickes*, 393 F.3d at 507. While Mr. Wyatt may have seemed nervous and uncomfortable, suspicious activity alone does amount to reasonable suspicion. *See Cortez*, 449 U.S. at 417. In the totality of the circumstances, Agent Ludgate lacked the reasonable suspicion necessary to commence the laptop search, thus constituting a violation of Ms. Koehler's privacy rights. Consequently, the Thirteenth Circuit properly reversed the lower court's denial of the Motion to Suppress.

In conclusion, non-routine border searches narrowly pass constitutional muster only where officers have reasonable, individualized suspicion. Here, not only did Agent Ludgate unreasonably believe the border search exception included laptop searches, but she also lacked the reasonable suspicion required to search Ms. Koehler's laptop, thus amounting to a Fourth Amendment privacy

violation. Accordingly, this Court should affirm the Thirteenth Circuit and suppress all evidence stemming from the Eagle City border station search.

II. THE USE OF THE PNR-1 DRONE AND DOPPLER RADAR CONSTITUTED A SEARCH IN VIOLATION OF THE FOURTH AMENDMENT.

The Thirteenth Circuit properly concluded that the use of the PNR-1 drone and Doppler radar device on Macklin Manor constituted impermissible searches in violation of Ms. Koehler's Fourth Amendment privacy rights. An unconstitutional search occurs when the government impedes an individual's reasonable expectation of privacy, defined as a subjective expectation that society deems reasonable. *Katz v. United States*, 389 U.S. 347 at 360–61 (Harlan, J., concurring); *see Kyllo v. United States*, 533 U.S. 27, 33 (2001). Notably, the advancement of technology and its use for invasive searches threatens the reasonable privacy guarantee. *See id.* at 34. To preserve the privacy rights enshrined in the Fourth Amendment, this Court must scrutinize any governmental use of invasive search technology. *See Kyllo*, 533 U.S. at 34; *California v. Ciraolo*, 476 U.S. 207, 211 (1986).

In this case, the warrantless use of a PNR-1 drone and Doppler radar to gather information from Macklin Manor were impermissible searches in violation of Ms. Koehler's Fourth Amendment rights. Subsequently, all resulting evidence constitute impermissible "fruits" that must be suppressed because, absent the information collected by these devices, the officers lacked probable cause for a search warrant.

A. The PNR-1 Drone Violated Ms. Koehler's Reasonable Expectation of Privacy Because the Area Searched was Curtilage Not Susceptible to Aerial Observation.

The Thirteenth Circuit properly held that the PNR-1 drone surveillance violated Ms. Koehler's reasonable expectation of privacy because the area searched falls within Macklin Manor's curtilage, and it is not susceptible to observation from a public aerial thoroughfare. A two-part inquiry determines whether an individual maintains a reasonable expectation of privacy:

(1) whether an individual manifests an actual, subjective expectation of privacy; and (2) whether society recognizes that expectation as reasonable. *Ciraolo*, 476 U.S. at 211; *see Smith v. Maryland*, 442 U.S. 735, 735 (1979); *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

The first part of the *Katz* inquiry asks whether an individual maintains a subjective intent to preserve something as private. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). This test does not require a significant showing of one's subjective expectation of privacy. *See, e.g.*, *Ciraolo*, 476 U.S. at 211–12 (denoting a privacy expectation by erecting a ten-foot fence around the area in question). *Cf. Alinovi v. Worchester Sch. Comm.*, 777 F.2d 776, 783 (1st Cir. 1985) (no subjective privacy expectation for term paper withheld from school principal when voluntarily given to other school officials). In this case, Ms. Koehler occupied a developed estate secluded in the outskirts of Eagle City, prevented her activities from open-air exposure, and did not readily consent to the observation of her property. *See* R. at 3–5; *Ciraolo*, 476 U.S. at 211–12. *Cf. Alinovi*, 777 F.2d at 1783. Thus, Ms. Koehler clearly demonstrated her subjective expectation of privacy.

Part two of the *Katz* inquiry objectively considers whether society is prepared to recognize an individual's subjective expectation of privacy as reasonable, based on societal values protected by the Fourth Amendment. *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *Oliver v. United States*, 466 U.S. 170, 181–83 (1984). Society grants upmost protection to areas immediately surrounding the home that extend "the intimate activity associated with the 'sanctity of a man's home and the privacies of life.'" *Oliver*, 466 U.S. at 180 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). These areas, known as the home's "curtilage," carry a reasonable, subjective expectation of privacy. *Id.* The "open fields doctrine" delineates the areas beyond the curtilage of a home where individuals lack legitimate privacy. *Dow Chemical Co. v. United States*, 476 U.S. 227, 235–36

(1986). In the context of aerial surveillance, a finding of one's reasonable privacy expectation only diminishes if the area is observable from a publicly-accessible airspace. *Ciraolo*, 476 U.S. at 213.

1. *The pool house and pool area fall within Macklin Manor's curtilage because of the estate's remote location, natural seclusion, and intimate activities.*

The Thirteenth Circuit properly held the pool house and pool area lied within Macklin Manor's curtilage because of the estate's remote location and intimate use. The nexus question for curtilage determinations is whether an area "is so intimately tied to the home itself that it should be placed under the home's umbrella of Fourth Amendment protection." *United States v. Dunn*, 480 U.S. 294, 301 (1987). The Court in *Dunn* uses four factors for this fact-specific analysis: (1) the proximity of the area to the home; (2) whether the area is within an enclosure surrounding the home; (3) the steps taken to avoid passerby observation; and (4) the nature of the area's use. *Id.*

A home's remote location directly influences three of the four key *Dunn* factors: proximity, the use of internal enclosures, and the steps taken to avoid passerby observation. *See United States v. Diehl*, 276 F.3d 32, 40 (1st Cir. 2002); *United States v. Reilly*, 76 F.3d 1271, 1279 (2d Cir. 1996). Proximity is generally relative based on the home's remoteness. *Compare Reilly*, 76 F.3d at 1279 (holding a cottage 375 feet from the rural main residence fell within the curtilage), *with United States v. Acosta*, 965 F.2d 1248, 1257 (3d Cir. 1992) (deeming an apartment complex backyard beyond the curtilage of a first floor city apartment). Additionally, remote homes may rely on natural enclosures to establish curtilage and ensure privacy protections, so long as no artificial internal enclosures further demarcate the property. *See Diehl*, 276 F.3d at 40 (finding a tent in a remote clearing with a forest perimeter did not need further artificial enclosures); *Daughenbaugh v. City of Tiffin*, 150 F.3d 594, 599 (6th Cir. 1998) (holding that a garage laid within the rural home's curtilage as demarcated by a river and tree coverage). *Cf. Bleavins v. Bartles*, 422 F.3d 445, 452 (7th Cir. 2005) (finding a barren field lay outside the home's curtilage

because it was separated by a gated fence, garage, and tool shed). Further, a remote home's surrounding terrain and natural enclosures accomplishes the goal of avoiding passerby observation as effectively as any artificial barrier, such as a roof or privacy fence. *See Diehl*, 276 F.3d at 41 (deeming the curtilage free from observation due to its remote location and enclosing woodland); *United States v. Jenkins*, 124 F.3d 768, 773 (6th Cir. 1997) (finding the home and curtilage avoids public view with its location within a wooded field in a lowly populated area).

When courts evaluate an area's use, they look for the presence of intimate activities expected within a home. *Dunn*, 480 U.S. at 300–02; *see Reilly*, 76 F.3d at 1278 (noting the use of a cottage and surrounding area for fishing, swimming, games, and cooking). *Cf. United States v. Traynor*, 990 F.2d 1153, 1157 (9th Cir. 2013) (finding a workshop's sole use to be the growth of marijuana and not for intimate activities of the home), *overruled on other grounds by United States v. Johnson*, 256 F.3d 895 (9th Cir. 2001) (en banc). Any objective information about the estate acquired by police officers should not abrogate a finding of intimate use if the officers acquired the information through an invasive search of the curtilage. *See Dunn*, 480 U.S. at 311 (Scalia, J., concurring).

In this case, Macklin Manor's remote location and intimate use permits inclusion of the pool house and pool area in the estate's curtilage. The pool house lies fifty feet from the main house to establish the outer limit of the estate's developed reach, thus satisfying the proximity factor. R. at 3; *see Reilly*, 965 F.3d at 1279. The estate does not utilize internal enclosures to separate the main house from the pool area. R. at 4; *see Bleavins*, 422 F.3d at 452. Mount Partridge provides an all-inclusive natural enclosure with cloud and fog cover to separate the property from external open areas. *See* R. at 4; *Diehl*, 276 F.3d at 40; *Daughenbaugh*, 150 F.3d at 599. Further, the natural enclosures trivialize the need for additional privacy barriers, as the estate's remoteness

and perennial low visibility prevent passerby observation and provide notice of expected privacy. *See* R. at 3–5; *Diehl*, 276 F.3d at 41; *Jenkins*, 124 F.3d at 773. Finally, residents use the pool house and pool area for occupancy and swimming activities. *See* R. at 4; *Reilly*, 76 F.3d at 1278–79. *Cf. Traynor*, 990 F.2d at 1157. The Doppler search necessitated a preceding invasion of the curtilage, and thus, the acquired information cannot abrogate the initial finding that the pool house lies within the estate's curtilage. *See Dunn*, 480 U.S. at 311 (Scalia, J., concurring). Therefore, Ms. Koehler's reasonable expectation of privacy extended through the full reach of Macklin Manor's curtilage, including both the pool house and pool area.

2. *Macklin Manor was not observable from a publicly-accessible airspace because of the estate's remote location and Mount Partridge's poor aerial visibility.*

The Thirteenth Circuit properly held that Macklin Manor was not susceptible to public aerial observation because the estate is remote, and poor aerial visibility makes overhead observation rare. A home's Fourth Amendment protections diminish if its activities are exposed to naked-eye view from a public thoroughfare. *Ciraolo*, 476 U.S. at 213. With aerial surveillance, police circumvent the warrant requirement when the home lies under a navigable airspace that is publicly available, routinely used, and legally accessible. *Id.* at 213–15; *see Florida v. Riley*, 488 U.S. 445, 450–452 (1989). The Court's development of this exception focuses excessively on the legal and regulatory permissibility of a search from a specific altitude or airspace. *See Florida*, 488 U.S. at 455 (O'Connor, J., concurring) ("[P]ublic use of altitudes . . . may be sufficiently rare that police surveillance from such altitudes would violate reasonable expectations of privacy, despite [regulatory] compliance . . . ."); *Ciraolo*, 476 U.S. at 213. While regulations need some evaluation, the Court must emphasize whether public use and observation from certain airspaces is common enough to render privacy expectations unreasonable. *See Florida*, at 460 (Brennan, J., dissenting) (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

The remoteness of a person's home and curtilage influences the reasonability of their expectation of privacy. For example, the Supreme Court of Vermont concluded that individuals choosing to live in a rural residence may possess a legitimate expectation of freedom from invasive aerial observation. *See State v. Bryant*, 950 A.2d 467, 478 (Vt. 2008). In contrast, courts find unreasonable privacy expectations from aerial surveillance when a home and curtilage fall within an area with routine and proximate flight paths. *See United States v. Breza*, 308 F.3d 430, 435 (4th Cir. 2002) (noting that low-altitude helicopter flights routinely occurred above the defendant's property); *United States v. Broadhurst*, 805 F.2d 849, 856 (9th Cir. 1986) (finding an airport's proximity to defendant's property diluted his expectation of privacy).

Courts distinguish homes observable by a passerby with the naked-eye from those only observable with a prolonged search with sense-enhancing technology. *See Dow Chemical Co.*, 476 U.S. at 238 n.5; *Ciraolo*, 476 U.S. at 213; *United States v. Taborda*, 635 F.2d 131, 139 (2d Cir. 1980). For example, the court in *Taborda* suppressed evidence derived from a sense-enhancing telescope not replicable with naked-eye observation. 635 F.2d at 139. *Cf. Dow Chemical Co.*, 476 U.S. at 238 n.5 (admitting pictures taken of a property with an aerial mapping camera with unenhanced visual quality similar to the naked eye); *Ciraolo*, 476 U.S. at 213 (admitting police observations with the naked eye from 1,000 feet above in a passing flight). It is also problematic when aerial surveillance occurs in a non-routine fashion without brevity, because it contravenes the permissible scope of aerial searches. *See Bryant*, 950 A.2d at 374 (citing *Ciraolo*, 476 U.S. at 213) (deeming it intrusive for a police helicopter to hover over a defendant's property for thirty minutes when trying to observe the home's activities).

In this case, the PNR-1 drone's aerial surveillance of Macklin Manor constituted an impermissible search. Macklin Manor's remote location on the outskirts of Eagle City supported

Ms. Koehler's expectation of being free from aerial surveillance. R. at 3; *see Bryant*, 950 A.2d at 478. The estate is extremely isolated and does not fall within a routinely used public flightpath. R. at 3, 42. In fact, aircrafts typically *avoid* the airspace because of the fog and cloud cover, further solidifying Ms. Koehler's expectation of privacy. R. at 3. *Cf. Breza*, 308 F.3d at 435; *Broadhurst*, 805 F.2d at 856. Similar to the telescope in *Taborda*, the PNR-1 drone used a sense-enhancing camera to obtain real-time, high definition photos and video with quality beyond that viewable with the naked eye. R. at 39; *see Taborda*, 635 F.2d at 139. *Cf. Dow Chemical Co.*, 476 U.S. at 238 n.5; *Ciraolo*, 476 U.S. at 213. Further, due to poor visibility, the drone had to hover over the property for an extensive fifteen minutes in order to obtain any information. R. at 41; *see Bryant*, 950 A.2d at 374. Finally, ambiguity of the drone's compliance with the 1640-foot altitude limit leads the surveillance further astray of the constitutional requirements of *Florida v. Riley*. *See* R. at 41; *Florida*, 488 U.S. at 451–52.

Therefore, because the pool house and pool area fell with Macklin Manor's curtilage, and because the estate was not susceptible to naked-eye observation from a public airspace, this Court must affirm that the PNR-1 drone search violated Ms. Koehler's reasonable expectation of privacy.

B. The Doppler Radar Search Violated Ms. Koehler's Privacy Rights Because the Radar Revealed Macklin Manor's Intimate Details and is Not in Common Use.

The Thirteenth Circuit properly held that the use of the Doppler radar on Macklin Manor was an unconstitutional search because it revealed the home's intimate details, and it is not in common use. The Fourth Amendment guarantees a reasonable expectation of privacy for the home. *Kyllo*, 533 U.S. at 34; *Katz*, 389 U.S. at 360–61. To solidify this guarantee, the Court uses a two-prong test to determine when the use of sense-enhancing technology amounts to an improper search: (1) the resulting information is otherwise unobtainable without physical intrusion; and (2) the technology is not generally in common use. *Kyllo*, 533 U.S. at 34.

The first *Kyllo* prong evaluates the intimate information gathered from a home via sense-enhancing technology and determines if physical intrusion would be the only alternative to obtain said information. *Id.* at 34, 37. Importantly, the Court finds that *all* details of the home are intimate details. *Id.* at 37; *see Florida v. Jardines*, 569 U.S. 1, 5–6 (2013) (extending privacy protections of the home to its respective curtilage). In *Kyllo*, the Court held that using thermal scanners to analyze a home's relative heating patterns is an invasive search because heating patterns are intimate details of the home otherwise unobtainable without actually being inside. *See Kyllo*, 533 U.S. at 37–39. The court in *Denson*, echoing the concerns raised in *Kyllo*, considered the use of a Doppler radar in finding technology that confirms the presence of someone within their own home constitutes a grave Fourth Amendment threat. *See United States v. Denson*, 775 F.3d 1214, 1218 (10th Cir. 2014). To avoid this concern entirely, courts require the obtained information show that only illegal activity occurred within the home, or that the homeowner did not confine the information to the interior of the home. *See Illinois v. Caballes*, 543 U.S. 405, 408–09 (2005) (admitting evidence from a drug dog search conclusively determining a car's only use was storing contraband); *United States v. Stanley*, 753 F.3d 114, 119–20 (3d Cir. 2014) (endorsing the use of a software tool to obtain information from a computer connected wirelessly to a neighbor's router because the owner did not confine the information to the home).

The second *Kyllo* prong finds the threat of sense-enhancing technology diminishes only when it has common usage, demonstrated by a showing of "general public use." *Kyllo*, 533 U.S. at 34, 40. To meet this standard, the technology must be available for public purchase, not just police use. *See id.* at 34 (finding a thermal imaging camera used by the police was not available for general public use). *Cf. Stanley*, 753 U.S. at 116 (concluding that a tracking software tool used by the police was publicly available on the manufacturer's website).

In this case, Detective Perkins's use of the Doppler radar device on Macklin Manor and its curtilage constituted an illegal search. Both Doppler searches revealed specific information about the number of individuals within the main house and pool house, along with their relative locations and positioning. R. at 4–5. Because this information is from within the home and curtilage, it receives the upmost privacy protection. *See Kyllo*, 533 U.S. at 37–39. Despite the lower court's assertion that the police could gather information on the number of people in the estate through non-invasive means, the individuals' physical location and positioning are intimate details not otherwise determinable without actual entry, as the details lacked outward manifestation. R. at 4–5; *see Kyllo*, 533 U.S. at 37–39; *Denson*, 775 F.3d at 1218. *Cf. Stanley*, 753 U.S. at 119–20. Additionally, the pool house search could not conclusively determine any illegal activity within. *See* R. at 5. While it showed three unmoving individuals and another *presumably* standing guard, absolute clarity required entry into the pool house. R. at 5. *Cf. Caballes*, 543 U.S. at 408–09.

Finally, the Doppler radar used to search the estate does not enjoy general public use. The device is manufactured specifically for police forces, it is unavailable for public purchase, and the average citizen has no reason to own one. R. at 35. *Cf. Stanley*, 753 U.S. at 116. Therefore, because the information gathered by the Doppler radar was otherwise unobtainable without entering the home, and because the Doppler radar does not enjoy common usage, this Court must affirm the Doppler radar search was unconstitutional.

C. Evidence From the PNR-1 Drone and Doppler Radar is Inadmissible Because the Border Search Did Not Provide Probable Cause to Search Macklin Manor.

The Thirteenth Circuit properly deemed the information gathered by the PNR-1 drone and Doppler radar searches impermissible "fruits" because the evidence from the border station could not establish probable cause to search Macklin Manor. The Fourth Amendment bars the use of evidence against a defendant secured through an illegal search, otherwise known as "fruits of the

poisonous tree." *Mapp v. Ohio*, 367 U.S. 643, 648 (1961). Permissibility requires proof of sufficient probable cause immediately preceding the questionable search. *Illinois v. Gates*, 462 U.S. 213, 232 (1983). Probable cause is a fluid concept that focuses on probabilities within specific contexts. *Maryland v. Pringle*, 540 U.S. 366, 370 (2003); *Gates*, 462 U.S. at 232. This standard applies factual and practical considerations of normal life relied on by reasonable people to determine, in the totality of the circumstances, whether an objective police officer would find probable cause to search for evidence of a crime in a specific location. *Ornelas v. United States*, 517 U.S. 690, 696 (1996); *Gates*, 462 U.S. at 230–31, 238.

Courts frequently reject the existence of probable cause for a warrant to search a home when the relied-on facts cannot establish a firm connection between evidence of a crime and the home. *See Poolaw v. Marcantel*, 565 F.3d 721, 733–34 (10th Cir. 2009); *United States v. Bethal*, 245 Fed. Appx. 460, 463 (6th Cir. 2007). For instance, the court in *Bethal* held that a search warrant for a defendant's home lacked probable cause when the supporting affidavit linked gun and drug dealing to a separate gang-controlled residence, but nothing linked the operations to the gang-affiliated defendant's personal residence. 245 Fed. Appx. at 463–66; *see also Poolaw*, 565 F.3d at 733–34 (10th Cir. 2009) (finding a lack of probable cause to search a home whose owners had a familial connection to the defendant but no involvement in his crimes).

In contrast, one circuit court found probable cause sufficient to search a residence that received telephone calls from the defendants' hotel rooms used for drug and theft operations, and from which phone calls were made to the police station inquiring about the defendants' arrests. *See United States v. Curry*, 911 F.2d 72, 75 (8th Cir. 1990). The court confirmed a fair probability that the police would find further evidence at the residence based on these communications, and

because the defendants stored the stolen property away from the hotel rooms, they fenced the property locally, and they obtained the drugs locally. *Id.*

In this case, the officers did not have probable cause to search Macklin Manor based on the border search. Similar to *Poolaw* and *Bethal*, the information obtained from the border station did not create the requisite connection between the suspected crime and Ms. Koehler's estate. *See Poolaw*, 565 F.3d at 733–34; *Bethal*, 245 Fed. Appx. at 463. Specifically, the border search revealed Mr. Wyatt's possession of $10,000 in $20 bills, the Ford family's personal information on Ms. Koehler's laptop, and Ms. Koehler's ownership of Macklin Manor. R. at 2–3. Unlike the residence in *Curry*, here the estate had no connection to the crime. *See* 911 F.2d at 75. The Macklin Manor deed records did not reveal the estate held the kidnappees; in fact, only the PNR-1 drone and Doppler radar searches could confirm that there was *anyone* at the estate. *See* R. 3–5.

Under the totality of the circumstances, the border search evidence lacked the objective sufficiency to conclude that probable cause existed to search Macklin Manor. Instead, the finding of probable cause required the information from the PNR-1 drone and Doppler radar searches. Therefore, because the PNR-1 drone wrongfully invaded Macklin Manor, and the Doppler radar impermissibly obtained intimate details of the estate, this Court should affirm the Thirteenth Circuit's decision to suppress the illicit "fruits" of the unconstitutional searches.

CONCLUSION

In sum, because the warrantless search at the Eagle City border station drastically exceeded the scope of the border search exception, and because the use of the PNR-1 drone and Doppler radar on Macklin Manor constituted searches unsupported by probable cause, the District Court erred in allowing evidence of these searches. This Court should affirm the decision of Court of Appeals for the Thirteenth Circuit to reverse and remand for further proceedings.