NEW YORK LAW SCHOOL

NYLS Law Review

Volume 64
Issue 2 *Spotlight on Student Scholarship*

Article 5

January 2020

United States v. Touset

Katelyn James
New York Law School

VOLUME 64 | 2019/20

KATELYN JAMES

United States v. Touset

64 N.Y.L. Sch. L. Rev. 207 (2019–2020)

ABOUT THE AUTHOR: Katelyn James is the Executive Notes and Comments Editor of the 2019–2020 *New York Law School Law Review*, J.D. candidate, New York Law School, 2020.

> *"Modern cell phones [are] now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."*
>
> —Chief Justice John G. Roberts Jr.[1]

Before the emergence of the digital age, carrying your most sensitive and personal information in your pocket was not the norm.[2] Today, with the digital age in full swing, not carrying a smartphone, or even a regular cell phone, has become the exception.[3] Smartphones track many aspects of our daily lives: the steps we take,[4] the calories we consume,[5] the photos we snap,[6] the money we spend,[7] and the people we connect with.[8]

Because of the quality and quantity of information we routinely store on our phones, serious individual privacy interests are implicated when law enforcement searches a digital device.[9] This concern is heightened at the U.S. border,[10] as most people travel with at least one digital device.[11] U.S. Customs and Border Protection (CBP) can search all persons and merchandise crossing the border pursuant to its authority to enforce immigration, customs, and federal laws.[12] These searches help

1. Riley v. California, 573 U.S. 373, 385 (2014).
2. *Id.* at 395.
3. *Id. See generally* Adam Fendelman, *How Are Cellphones Different From Smartphones?*, Lifewire (Oct. 14, 2019), https://www.lifewire.com/cell-phones-vs-smartphones-577507 (distinguishing a cellphone from a smartphone, as a cellphone can make and receive phone calls and text messages while a smartphone can make and receive phone calls and text messages, surf the internet, and download applications).
4. *See* Brad Jones, *6 Things You Didn't Realize Your iPhone is Tracking*, Make Use Of (June 21, 2017), https://www.makeuseof.com/tag/iphone-tracking/.
5. David LaGesse, *Lose Weight With Your Phone*, AARP (Apr. 14, 2011), https://www.aarp.org/health/fitness/info-04-2011/lose-weight-with-your-phone.html.
6. David Nield, *All the Ways Your Smartphone and Its Apps Can Track You*, Gizmodo (Sept. 12, 2019), https://gizmodo.com/all-the-ways-your-smartphone-and-its-apps-can-track-you-1821213704.
7. Ryan Dezember, *Your Smartphone's Location Data Is Worth Big Money to Wall Street*, Wall St. J. (Nov. 2, 2018), https://www.wsj.com/articles/your-smartphones-location-data-is-worth-big-money-to-wall-street-1541131260.
8. *See* Nield, *supra* note 6.
9. United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013).
10. *Id.* at 961 (noting that airports with international terminals, along with all ports of entry, are considered the functional equivalent of the border).
11. United States v. Kolsuz, 890 F.3d 133, 145 (4th Cir. 2018).
12. *Privacy Impact Assessment: Update for CBP Border Searches of Electronic Devices*, Dep't of Homeland Sec. 1 (2018), https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf.

detect evidence of child pornography, digital contraband,[13] human trafficking, terrorism, and commercial crimes.[14]

This Case Comment contends that the court in *United States v. Touset* erred when it held that no standard of suspicion is required to conduct forensic searches of electronic devices at the U.S. border.[15] First, the *Touset* court failed to consider relevant precedent, including its own precedent, that held reasonable suspicion is the standard required at the border to uphold a forensic search of electronic devices.[16] Second, the *Touset* court misapplied binding Supreme Court precedent[17] when it failed to consider electronic devices as a new "category of effects."[18] The *Touset* court's decision jeopardizes the privacy interests of every American who travels internationally, and does very little to achieve the CBP's goals to secure the border.[19]

In September 2014, Xoom, a money transmitting company, identified several individuals who made frequent payments to accounts located in countries known for sex trafficking and child pornography.[20] The Xoom users utilized Yahoo! e-mail addresses to create their Xoom accounts,[21] which prompted Xoom to alert the National Center for Missing and Exploited Children (NCMEC) and Yahoo!.[22] Upon further investigation, Yahoo! discovered that one of the e-mail accounts[23] contained a file with child pornography.[24] Yahoo! sent this information to the NCMEC, who then notified the Department of Homeland Security (DHS).[25] DHS subpoenaed several money transmitting companies, including Western Union, in an effort to

13. Digital contraband is any computer file that, outside very specific authorized exceptions, cannot be legally possessed. Michael Adler, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 Yale L.J. 1093, 1097 (1996).

14. *Border Search of Electronic Devises*, U.S. Customs and Border Prot. (Jan. 4, 2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.

15. 890 F.3d 1227, 1231 (11th Cir. 2018).

16. United States v. Vergara, 884 F.3d 1309, 1313 (11th Cir. 2018).

17. Riley v. California, 573 U.S. 373, 402–03 (2014).

18. *Touset*, 890 F.3d at 1233.

19. *Compare Vergara*, 884 F.3d at 1317 (Pryor, J., dissenting), *with Touset*, 890 F.3d at 1236. The *Touset* court's ruling sacrifices privacy protections under the Fourth Amendment with little benefit—digital contraband is often stored on cloud storage, backup servers, or on other devices, and thus, has the potential to be forever present. *Touset*, 890 F.3d at 1236.

20. United States v. Touset, No. 1:15-CR-45-MHC, 2016 U.S. Dist. LEXIS 31666, at *1–3 (N.D. Ga. Mar. 11, 2016). Countries known for sex trafficking and child pornography include the Philippines, Thailand, and the Dominican Republic. *Id.* at *2.

21. *Id.* at *2.

22. *Id.*

23. The e-mail account "ilovyousomuch0820@yahoo.com" was connected to defendant Touset. *Id.*

24. *Id.* The e-mail account also listed a phone number linked to the Philippines. *Id.*

25. *Id.* The NCMEC notifies the DHS Cyber Crime Center of suspicious activity. *See Reporting Crime*, USA.Gov, https://www.usa.gov/report-crime (last visited Mar. 25, 2020).

retrieve the transactions linked to the implicated Yahoo! e-mail account.[26] Western Union discovered that defendant Karl Touset maintained an account that listed three payments in amounts ranging from thirty-five to thirty-seven dollars between March and July 2013.[27]

On December 21, 2014, Touset was stopped at the airport in Atlanta, Georgia, as he returned to the United States from the Netherlands.[28] CBP agents searched his bags and electronic devices that included a camera, two iPhones, laptops, tablets, and external hard drives.[29] A CBP agent manually searched the camera and the two iPhones at the scene, and when the search did not uncover anything incriminating, returned these devices to Touset.[30] However, CBP seized the external hard drives, tablets, and laptops for seventeen days and sent them to an off-site DHS lab for further investigation.[31]

DHS forensic analysts searched Touset's seized devices and discovered child pornography on his laptops and external hard drives.[32] Due to this discovery, DHS agents obtained a search warrant for Touset's home.[33] Based on the evidence obtained during the execution of the search warrant,[34] a grand jury indicted Touset in 2015 on three counts associated with receiving, transporting, and possessing child pornography.[35] Touset pleaded not guilty and filed motions to suppress the evidence[36] obtained during the search of his devices.[37]

The District Court for the Northern District of Georgia, Atlanta Division, denied Touset's motions to suppress and based its holding on the 2013 case, *United States v. Cotterman*, where the court held that reasonable suspicion is required for forensic searches of electronic devices at the border.[38] Applying this standard, the

---

26. *Touset*, 2016 U.S. Dist. LEXIS 31666, at *2–3.

27. *Id.* at *3.

28. *Id.* at *3–4.

29. *Id.*

30. *Id.* at *4.

31. *Id.* at *5–6. Touset was free to leave after thirty minutes. *Id.* at *5.

32. *Id.* at *4.

33. *Id.* Touset was read his *Miranda* rights during the execution of the search warrant. *Id.*

34. United States v. Touset, 890 F.3d 1227, 1230–31 (11th Cir. 2018). Between 2013 and 2015, Touset sent more than $55 thousand to the Philippines. *Id.* He purchased thousands of images and webcam sessions with underage girls. *Id.* Each transaction ranged from thirty-five to one hundred dollars. *Id.*

35. *Id.* at 1231. The three counts Touset was charged with were (1) knowingly receiving child pornography, (2) knowingly transporting and shipping child pornography, and (3) knowingly possessing a computer storage device containing child pornography. *See id.*

36. A motion to suppress evidence is a pre-trial motion in which the defendant asks the judge to suppress the evidence at trial because it is inadmissible. *See generally* Fed. R. Crim. P. 12(b)(3)(c).

37. *Touset*, 890 F.3d at 1231.

38. 709 F.3d 952, 962 (9th Cir. 2013). The court in *Cotterman* defined reasonable suspicion as "a particularized and objective basis for suspecting the particular person stopped of criminal activity." *Id.*

district court reasoned that the CBP agents had reasonable suspicion to search Touset's electronic devices, and denied his motions.[39] Touset appealed to the Eleventh Circuit Court of Appeals, which held that the Fourth Amendment does not require any level of suspicion before conducting a forensic search of electronic devices seized pursuant to a border search.[40] The Eleventh Circuit held in the alternative that reasonable suspicion existed to support the forensic search of Touset's electronic devices, should some level of suspicion have been required.[41]

Fourth Amendment jurisprudence has long been characterized as yielding "doctrinal incoherence," and legal experts have increasingly showed renewed interest in the Framers' original intent.[42] In the 1967 foundational Fourth Amendment case *Katz v. United States,* the Supreme Court held that warrantless searches are generally unlawful, subject to only a few "specifically established and well-delineated exceptions."[43] Fourth Amendment jurisprudence has developed to recognize border stops as one of the well-delineated exceptions given the high governmental interest in protecting the borders and enforcing U.S. law.[44] The border exception rests on the idea that one's expectation of privacy is lower at the border of our nation than within it, because a "port of entry is not a traveler's home."[45]

Border searches are classified into two types: routine and non-routine.[46] A routine border search is deemed reasonable because it occurs at the border and

at 968. The assessment is made in light of the totality of the circumstances, and factors which may have an innocent explanation can collectively amount to reasonable suspicion. *Id.*

39. *Touset*, 2016 U.S. Dist. LEXIS 31666, at *12.

40. *Touset*, 890 F.3d at 1227.

41. *Id.* at 1237.

42. *See, e.g.*, David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 U. Pa. J. Const. L. 581, 581–83 (2008) (discussing the main differences between the three common interpretations used by lawyers and scholars of the Fourth Amendment); Barry Friedman & Orin Kerr, *The Fourth Amendment*, Nat'l Const. Ctr., https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv (last visited Mar. 25, 2020) (discussing the debate on the Fourth Amendment's protection for incidents such as surveillance and police tactics).

43. 389 U.S. 347, 356–67 (1967). Under Fourth Amendment jurisprudence, a search warrant is generally required for a search to be constitutional. *See generally* Illinois v. Rodriguez, 497 U.S. 177 (1990) (holding a warrantless search does not violate the Fourth Amendment if police reasonably believe the person who consented to the search had the authority to do so); United States v. Martinez-Fuerte, 428 U.S. 543 (1976) (holding that routine checkpoints are reasonable at the border); Carroll v. United States, 267 U.S. 132 (1925) (establishing the automobile exception to the warrant requirement of the Fourth Amendment).

44. United States v. Montoya de Hernandez, 473 U.S. 531, 537–38 (1985).

45. United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005).

46. The distinction between routine and non-routine border searches has turned on the level of intrusiveness. *See, e.g.*, United States v. Johnson, 991 F.2d 1287, 1291–92 (7th Cir. 1993) ("When a border search and seizure becomes nonroutine, a customs official needs reasonable suspicion to justify it."); *Montoya de Hernandez*, 473 U.S. at 540–41 (explaining the relationships between the reasonable suspicion standard and the level of intrusiveness of a search). However, the Supreme Court has suggested that the distinction between routine and non-routine searches may no longer apply to searches of vehicles and

consists of only a limited intrusion.[47] A non-routine border search requires reasonable suspicion because it varies in technique and is generally more intrusive.[48] The Supreme Court has held that only routine border searches are granted the full extent of the border search exception to the warrant requirement of the Fourth Amendment.[49] Conversely, non-routine searches must rest on some "articulable degree of particularized suspicion" based on the scope of the search.[50]

While the Supreme Court has yet to squarely address the narrow intersection between the Fourth Amendment and modern technology at the border, it has provided helpful guidance.[51] In 2014, the Court in *Riley v. California* unanimously struck down the warrantless search of the digital information stored on a cell phone that was part of a search incident to an arrest.[52] Further, in 2018, the Court in *Carpenter v. United States* held that the warrantless access to cell-site information, which linked the defendant to a series of armed robberies, violated the Fourth Amendment.[53]

Lower courts have relied on the precedent set forth in *Riley* and *Carpenter* to address warrantless searches of electronic devices—creating a circuit split between the Fourth and Eleventh Circuits.[54] In *United States v. Kolsuz,* the Fourth Circuit court held that the warrantless forensic analysis of the defendant's phone was

personal property at the border. *See generally* United States v. Flores-Montano, 541 U.S. 149, 152 (2004) (finding that the complex balancing tests utilized to determine what is routine versus intrusive in the context of a search of a person at the border should not be extended to cover searches of vehicles at the border).

47. *See Johnson*, 991 F.2d at 1290–92.

48. Yule Kim, Cong. Research Serv., RL31826, Protecting the U.S. Perimeter: Border Searches Under the Fourth Amendment 10–11 (2009).

49. *Montoya de Hernandez*, 473 U.S. at 538.

50. *Id.* at 541. In *Montoya de Hernandez,* the Supreme Court required reasonable suspicion for the first time in the border context for a defendant who was suspected of smuggling drugs in her alimentary canal. *Id.* However, searches of people and property are generally limited to the physical confines of the individual being searched and their items. *See* Riley v. California, 537 U.S. 373, 383 (2014). When a person is searched incident to arrest, the searches have been narrowed to the area within the arrestee's immediate control for the purposes of ensuring an arrestee cannot access a weapon and preserving evidence. *See* Chimel v. California, 395 U.S. 752, 762–63 (1969).

51. *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018); *Riley*, 573 U.S. at 373.

52. *Riley*, 573 U.S. at 386–87. The electronic data could not be used as a weapon to harm the officers, to assist in escape during arrest, or for the destruction of evidence, which have been the main reasons for the search incident to arrest exception. *See id.* at 383 (citing United States v. Robinson, 414 U.S. 218, 235 (1973)).

53. *Carpenter*, 138 S. Ct. at 2219. Cell phones connect to radio antennas, known as cell-sites, that have several directional antennas dividing a covered area into sectors. *Id.* at 2211–12. Cell phones operate by scanning the environment in search of the nearest cell-site to get the strongest signal. *Id.* Each time a cell phone connects to a cell-site, it creates a time-stamped cell-site location information (CSLI) record. *Id.* The accuracy of the CSLI is determined by the size of the coverage area. *Id.* The smaller the coverage area, the more cell-sites there are and thus, greater accuracy of the CSLI. *Id.* Urban areas have many cell-sites to handle the increased use of cell phones. *Id.*

54. *Compare* United States v. Kolsuz, 890 F.3d 133, 148 (4th Cir. 2018) (concluding that it was reasonable for officers to conduct a search of an electronic device based on having "at least" reasonable suspicion),

constitutional under the border search exception because the officers had "at least" reasonable suspicion for the search.[55] In the Eleventh Circuit, *Touset* joined the discussion by holding—albeit incorrectly—that warrantless forensic searches of electronic devices at the border do not require any level of suspicion.[56]

In 2019, the Ninth Circuit Court of Appeals, in *United States v. Cano*, clarified *Cotterman*, holding that "reasonable suspicion" in the context of searching electronic devices at the border means that agents must reasonably suspect digital contraband on the device.[57] *Cano* distinguishes manual cell phone searches at the border from forensic searches, holding that cell phones can be manually searched by border officials without reasonable suspicion, but forensic searches of cell phones require reasonable suspicion.[58] In *Cano*, the Ninth Circuit Court of Appeals makes it clear that all searches of cell phones at the border must be limited in scope to searching for digital contraband.[59]

In his appeal of the trial court's denial of his motions, Touset argued that the court erred in its decision because under *Riley*, reasonable suspicion was required to forensically search his devices.[60] The government argued that it did not need reasonable suspicion to search his devices because the search was not an invasive physical search.[61] Further, the government argued that *Riley* does not apply to searches at the border.[62] The Eleventh Circuit held that no standard of suspicion was required for searches of electronic devices at the border and reasoned that the search incident to arrest exception in *Riley* does not apply to border searches because "property and persons are different."[63] In the alternative, the court held the government had reasonable suspicion that Touset possessed child pornography due to the tips DHS received from private organizations.[64] The concurring opinion in *Touset* agrees only in the judgment of the court's alternative ruling.[65] In his

with United States v. Touset, 890 F.3d 1227, 1231 (11th Cir. 2018) (stating that the Fourth Amendment does not require any level of suspicion for searches of electronic devices at the border).

55. *Kolsuz*, 890 F.3d at 147–48.

56. *Touset*, 890 F.3d at 1229.

57. 934 F.3d 1002, 1007 (9th Cir. 2019).

58. *Id.*

59. *Id.*

60. *Id.*

61. Brief for Appellee at 19, United States v. Touset, 890 F.3d 1227 (11th Cir. 2018) (No. 17-11561-DD). The government also argued that it had reasonable suspicion to search Touset in the first place. *Id.*

62. *See id.* at 27–33.

63. United States v. *Touset*, 890 F.3d 1227, 1234 (11th Cir. 2018). The *Touset* court reasoned that Supreme Court precedent "considers only the 'personal indignity' of a search, not its extensiveness . . . [and] [it] fail[ed] to see how the personal nature of data stored on electronic devices could trigger this kind of indignity when . . . precedent establishes that a suspicion-less search of a home at the border does not." *Id.*

64. *Id.* at 1237.

65. *Id.* at 1239 (Corrigan, J., concurring).

concurrence, Judge Timothy Corrigan reasoned that because, in this instance, CBP had reasonable suspicion of criminal activity, the court did not need to reach the "new-found government position" that border agents do not need any justification to forensically search devices at the border to decide the case.[66]

The Eleventh Circuit erred when it held that no reasonable suspicion was required to forensically search Touset's electronic devices.[67] First, the *Touset* court failed to follow relevant precedent, including its own precedent, that held reasonable suspicion as the standard required at the border to allow warrantless forensic searches of electronic devices.[68] As announced by the Eleventh Circuit's 2018 opinion in *United States v. Vergara*, the level of suspicion required at the border is reasonable suspicion.[69] Even at the border, the nature and scope of any search must be balanced against the Fourth Amendment's reasonableness requirement.[70]

Not only did the Eleventh Circuit fail to adhere to its own precedent, it also ignored relevant Supreme Court precedent in formulating its decision.[71] The Supreme Court has held that warrantless searches are unreasonable under the Fourth Amendment if they uncover intrusive and sensitive information.[72] In 1985, the Court, in *Montoya de Hernandez,* held that reasonable suspicion was required for the search of the traveler's alimentary canal as such search went beyond the scope of a routine border search.[73] In the 2001 case, *United States v. Kyllo*, the Court held that thermal-imaging devices used to track heat emanating from within a home went beyond the reasonable expectation of privacy because the devices are not within general public use, and the information obtained would not have been accessible without physical intrusion into the home.[74] In 2018, the *Carpenter* Court held the

66. *Id.* at 1238–39 (Corrigan, J., concurring).

67. *Id.* at 1231.

68. *See* United States v. Vergara, 884 F.3d 1309, 1313 (11th Cir. 2018) ("[W]e need not—and do not—address the questions whether reasonable suspicion was required for the searches or whether reasonable suspicion existed.").

69. *Id.*

70. United States v. Cotterman, 709 F.3d 952, 960 (2013). *See generally* Terry v. Ohio, 392 U.S. 1, 21–22 (1968) (establishing that the reasonableness of any specific search and seizure under the Fourth Amendment must be assessed in light of the particular circumstances against the standard of whether a person of reasonable caution is warranted in believing that the action taken was appropriate).

71. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (holding that the defendant's reasonable expectation of privacy was invaded when the government accessed his cell phone data); Riley v. California, 573 U.S. 373, 386 (2014) (holding that officers must obtain a warrant to search cell phones); *Touset*, 890 F.3d at 1234 (discussing and ultimately distinguishing the instant case from other courts' holdings relating to cell phone searches).

72. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2219; *Riley*, 573 U.S. at 386; United States v. Jones, 565 U.S. 400, 404 (2012); Kyllo v. United States, 533 U.S. 27, 34 (2001).

73. United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985). The Court acknowledged that some searches are "particularly offensive," and thus require particularized suspicion. *Id.* at 542.

74. 533 U.S. 27, 34 (2001). In 2001, the Court recognized that "the rule we adopt must take account of more sophisticated systems that are already in use or in development." *Id.* at 36.

warrantless access of cell-site location data violated the Fourth Amendment because there is a recognized reasonable expectation of privacy in one's movement and location.[75]

The Ninth and Fourth Circuits have held that reasonable suspicion is required before conducting forensic searches of electronic devices at the border.[76] The Ninth Circuit reasoned that reasonable suspicion is required because of the "comprehensive and intrusive nature" of a forensic search.[77] In *Kolsuz*, the Fourth Circuit upheld the constitutionality of a search of an iPhone at the border because it was based on "at least reasonable suspicion."[78]

There are stark differences between the nature of the data uncovered during the searches of Touset's devices, and that of the searches in *United States v. Jones*, *Carpenter*, *Riley*, and *Kyllo*.[79] In *Jones* and *Carpenter*, only Global Positioning System (GPS) or cell-site information, respectively, were uncovered in the challenged searches.[80] In both cases, the Court held that warrantless disclosure of location information—whether through cell-site data or GPS information—violated the Fourth Amendment.[81] In *Riley,* only photos and videos were taken from a cell phone—nonetheless, the Court held that the search violated the Fourth Amendment.[82] Finally, in *Kyllo*, the Court held a search unconstitutional because it revealed the temperature emanating from the interior of a home.[83] None of these cases uncovered nearly the same amount—or type—of personal and sensitive information that was uncovered in *Touset*—yet in all these cases, the Supreme Court required a warrant for the search.[84]

At a minimum, reasonable suspicion should be required to search an electronic device because a warrantless forensic search provides access to a vast amount personal

75. *Carpenter*, 138 S. Ct. at 2219.

76. United States v. Cano, 934 F.3d 1002, 1015 (9th Cir. 2019); United States v. Kolsuz, 890 F.3d 133, 148 (4th Cir. 2018).

77. United States v. Cotterman, 709 F.3d 952, 962 (9th Cir. 2013). The *Cotterman* court analogized the forensic search of electronic devices to a strip search, calling it a "computer strip search" due to the intrusiveness and the degree of indignity that follows because of the personal and intimate details stored on electronic devices. *Id.* at 966.

78. *Kolsuz*, 890 F.3d at 148. In *Cano*, the court extended this reasoning to apply equally to cell phones. *Cano*, 934 F.3d at 1015.

79. *Carpenter*, 138 S. Ct. at 2219; Riley v. California, 573 U.S. 373, 378–79 (2014); United States v. Jones, 565 U.S. 400, 403–04 (2012); *Kyllo*, 533 U.S. at 34–35.

80. *Jones*, 565 U.S. at 403 (holding that the attachment of a GPS to the defendant's vehicle, and subsequent use of that device to monitor the vehicle's movement, constituted a search under the Fourth Amendment); *Carpenter*, 138 S. Ct. at 2212 (holding that the government's acquisition of the defendant's cell-site records constituted a search under the Fourth Amendment).

81. *Id.* at 2219; *Jones*, 565 U.S. at 404.

82. *Riley*, 573 U.S. at 403.

83. *Kyllo*, 533 U.S. at 38–39.

84. *Carpenter*, 138 S. Ct. at 2221; *Riley*, 573 U.S. at 386; *Jones*, 565 U.S. at 404; *Kyllo*, 533 U.S. at 40.

and sensitive information.[85] Thus, individuals have an expectation of privacy in their electronic devices because they contain such information.[86] In *Touset*, the CBP agents had access to many of Touset's devices: cell phones, a camera, two laptops, two tablets, and two hard drives.[87] Taken together, unfettered access to these devices painted a near-complete—and invasive—portrait of Touset's personal life.[88]

Reasonableness has been recognized as the touchstone for warrantless searches under the Fourth Amendment.[89] It is unreasonable to find, as *Touset* did, that no suspicion is required for the seizure and forensic search of an individual's electronic devices merely because the search takes place at the border.[90] Reasonable suspicion should be the standard applicable to forensic searches of devices at the border due to the intrusive nature of the search and the type of information that will inevitably be uncovered.[91] Had the Eleventh Circuit followed relevant precedent, including its own, it would have recognized that reasonable suspicion was required to conduct the search of Touset's electronic devices.

The second error of the *Touset* court was that it misapplied precedent set forth by the Supreme Court in *Riley*. The *Touset* court failed to consider electronic devices as a different "category of effects" when determining whether the border search exception applies to the warrant requirement.[92] Instead, the *Touset* court held that electronic devices are the same as other property under the Fourth Amendment.[93]

The Supreme Court, in determining whether an existing exception to the warrant requirement applies to a particular "category of effects," has held that courts must balance individual privacy interests against governmental interests.[94] *Riley* categorized personal electronic devices as a new "category of effects" that must be considered when weighing individual privacy interests against government interests in determining whether an exception to the Fourth Amendment's warrant requirement exists.[95] In *Riley*, the Court reasoned that modern cell phones are a "category of effects," fundamentally different than other objects traditionally subjected to a

85. United States v. Cotterman, 709 F.3d at 952, 965–66 (9th Cir. 2013).

86. *Id.* at 965. Electronic devices have immense storage capabilities, and can store vast amounts of personal and sensitive information. *Id.*

87. United States v. Touset, 890 F.3d 1227, 1230 (11th Cir. 2018).

88. *See generally id.* (detailing all of the evidence discovered on Touset at the point of entry into the United States).

89. *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (citing Flippo v. West Virginia, 528 U.S. 11, 13 (1999)); Ohio v. Robinette, 519 US 33, 39 (1996); Florida v. Jimeno, 500 U.S. 248, 250 (1991); Katz v. United States, 389 U.S. 347, 357 (1967).

90. *Touset*, 890 F.3d at 1233.

91. United States v. Cano, 934 F.3d 1002, 1015 (9th Cir. 2019) (citing *Cotterman*, 709 F.3d at 968).

92. *Touset*, 890 F.3d at 1234.

93. *Id.*

94. *See* Riley v. California, 573 U.S. 373, 391 (2014).

95. *See id.* at 386.

search, and thus, cannot be fairly compared when considering the privacy interests implicated during a search.[96] The Court provided two rationales for its characterization: (1) the quantitative difference due to the amount of information stored on electronic devices,[97] and (2) the qualitative difference due to the pervasiveness of the search.[98] The Court further reasoned that before electronic devices existed, privacy implications of property were limited to the physical realities of what was being searched.[99]

A modern personal electronic device contains more sensitive information than what would historically—and even quite recently—have been found as the result of the search of an individual's person and effects.[100] Accordingly, searches of personal electronic devices might expose more information to the government than even an exhaustive search of a home,[101] where privacy is "most heightened."[102] The *Riley* Court considered the nature of the devices themselves and concluded that electronic devices are not just another "technological convenience"[103] and, because the information stored on a cell phone reflects the intricacies of private life, warrantless digital searches are a significant diminution of privacy.[104] Had the Eleventh Circuit followed the reasoning outlined in *Riley*, it would have found that personal electronic devices belong in a different "category of effects" than other physical items when considering whether the Fourth Amendment's warrant exception applies.[105]

Several circuit courts have interpreted *Riley* in a border context.[106] In the 2015 case, *United States v. Jae Shik Kim,* the D.C. Circuit court held that *Riley* had created a new Fourth Amendment balancing test for the search of electronic devices at the border by "assessing, on the one hand, the degree to which the search intrudes upon an individual's privacy, and, on the other, the degree to which it is needed for the

96. *See id.* at 396–97.

97. *Riley* acknowledges the immense storage capacity on devices such as phones, laptops, and tablets. *Id.* at 393–94. This includes "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.*

98. *Id.* at 375. The information stored on a device collects, in one place, data that reveals more than any isolated record. *Id.* The information stored includes photos, texts, calendar events, phone books, internet history, and historical location data. *Id.* at 393–94.

99. *Id.*

100. *Id.* at 395.

101. *Id.* at 396–97.

102. California v. Ciraolo, 476 U.S. 207, 212–13 (1986) (holding that expectations of privacy are the most heightened in the home). *Riley* rejected the argument that a search of cell phone data should be treated the same as a search of other physical items, stating, "that is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley*, 573 U.S. at 393.

103. *Riley*, 573 U.S. at 403.

104. *Id.* at 393–94.

105. *Id.* at 398–99.

106. *See, e.g.*, United States v. Kolsuz, 890 F.3d 133, 146 (4th Cir. 2018); United States v. Jae Shik Kim, 103 F. Supp. 3d 32, 55 (D.D.C. 2015).

promotion of legitimate governmental interests."[107] In the Fourth Circuit, the court in *Kolsuz* found that *Riley* confirms the rationale that forensic searches of electronic devices should be characterized as non-routine border searches that require some form of individualized suspicion.[108]

In *Vergara*—the 2018 case immediately preceding *Touset*—the court found that *Riley* did not apply to border searches.[109] The court reasoned that the holding in *Riley* did not impact border searches because they have generally been exempt from the warrant and probable cause requirements under the Fourth Amendment.[110] Although bound by *Vergara*'s narrow interpretation of *Riley*, *Touset* misapplied the binding *Riley* precedent that electronic devices are not in the same category as other property, or persons, when determining whether the warrant exception applies under the Fourth Amendment.[111] Instead, the *Touset* court relied on inapplicable precedent of physical searches at the border and thus, held that electronic device searches are the equivalent to other property searches under the Fourth Amendment.[112]

The *Touset* court relied on precedent that focused on physical searches at the border to support its reasoning that privacy interests are not implicated during a forensic search of electronic devices.[113] The *Touset* court used three factors to determine the intrusiveness of a search at the border: (1) the contact between the officer and the person being searched; (2) exposure of intimate body parts, and (3) the use of force.[114] However, these factors do not address the totality of issues involved in searches of electronic devices because they are limited to the physical intrusiveness of a search, and not the nature of the information uncovered.[115] The *Touset* court compares the forensic search of devices to other travel indignities, such as the forced removal of shoes, and walking through an electronic body scanner.[116] But under the *Riley* framework, these physical searches are not analogous to those in *Touset* because modern electronic devices implicate privacy interests on a far greater scale.[117]

107. *Jae Shik Kim*, 103 F. Supp. 3d at 55. In *Jae Shik Kim*, the defendant's motion to suppress the evidence uncovered during a forensic search of his laptop was granted after the court held the search was unreasonable without any form of suspicion, and because the search was "so invasive of [the defendant's] privacy and so disconnected from not only the considerations underlying the breadth of the government's authority to search at the border, but also the border itself." *Id.* at 59.

108. *Kolsuz*, 890 F.3d at 147.

109. United States v. Vergara, 884 F.3d 1309, 1312–13 (11th Cir. 2018).

110. *Id.*

111. United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018).

112. *Id.*

113. *Id.* (citing United States v. Vega-Barvo, 729 F.2d 1341, 1346 (11th Cir. 1984)).

114. *Touset*, 890 F.3d at 1234.

115. The *Touset* court relies on *Vega-Barvo* for factors to determine intrusiveness of a search; however, the court does not consider the personal privacy interests that arise for the search of property when applying to the specific facts of Touset's case. *Id.*

116. *Id.* at 1235.

117. Riley v. California, 573 U.S. 373, 393 (2014).

Further, the *Touset* court rejected categorizing electronic devices as anything other than property because they store vast amounts of personal information.[118] The *Touset* court's refusal to categorize electronic devices as anything other than property because they are used by many people conflicts with the rationale in *Riley*.[119] In *Riley*, the Court outlined that cell phones are a different "category of effects" because they are a ubiquitous and vital part of daily life and thus, require additional considerations when determining if the border exception to the warrant requirement applies.[120] The single cell phone searched in *Riley* was a 2009 model and offered significantly less storage capabilities than present-day phones.[121] In *Touset*, the search encompassed two iPhones, a camera, two laptops, two tablets, two hard drives, and thus, a correspondingly higher amount of personal data than in *Riley*.[122] The *Touset* court's focus on only the personal indignity of the search, and not its extensiveness,[123] directly conflicts with *Riley*'s rationale for distinguishing electronic devices from other items at the border.[124]

The Eleventh Circuit hosts the world's busiest airport, Atlanta-Hartsfield-Jackson, which enplanes and deplanes about 104 million passengers a year.[125] The Ninth Circuit hosts the seventh busiest airport in the world, Los Angeles International Airport.[126] The Fourth Circuit hosts two of America's busiest airports: Charlotte/Douglas International Airport and Baltimore-Washington International Thurgood Marshall Airport.[127] The circuit split on the standard of suspicion required to conduct forensic searches of electronic devices poses problems given the high traveler rates at these airports.[128] The Eleventh Circuit's decision[129] not to find any standard of suspicion required for the forensic searches of devices at the border creates inherent privacy issues for U.S. citizens who travel anywhere by air, and is ineffective for

118. *Touset*, 890 F.3d at 1233.

119. *Id.*

120. *Riley*, 573 U.S. at 384–85.

121. *Id.* at 378–79.

122. *See generally Touset*, 890 F.3d at 1230; *Riley*, 573 U.S. at 373. Computer storage capacities tend to double every two years. Carla Tardi, *Moore's Law Explained*, Investopedia (Sept. 5, 2019), https://www.investopedia.com/terms/m/mooreslaw.asp.

123. *Touset*, 890 F.3d at 1234.

124. *Riley*, 573 U.S. 376.

125. *CI World Releases Preliminary 2017 World Airport Traffic Rankings Passenger Traffic,* Airports Council Int'l (Apr. 9, 2018), https://aci.aero/news/2018/04/09/aci-world-releases-preliminary-2017-world-airport-traffic-rankings-passenger-traffic-indian-and-chinese-airports-major-contributors-to-growth-air-cargo-volumes-surge-at-major-hubs-as-trade-wars-thre.

126. *Id.*

127. Melanie Renzulli, *The 25 Busiest Airports In The United States*, Trip Savvy (June 26, 2019), https://www.tripsavvy.com/busiest-airports-in-the-usa-3301020.

128. *See generally id.*

129. United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018).

curtailing the transfer, use, and purchase of digital contraband, such as child pornography.[130]

The information accessed during a forensic search of electronic devices is often of a far more sensitive, private, and thus intrusive nature, than information gleaned through searches of traditional physical items.[131] For example, it is unlikely that a person would bring with them a printout of their entire internet search history, credit card statements, tax documents, photo albums, and personal phone books each time they travel.[132] However, when individuals travel with their cell phones, they carry all of this information with them—perhaps more.[133] A forensic search not only brings to the surface what is currently stored on the device, but can also recover past browsing history and restore long discarded information.[134] Should other circuits decide to follow the Eleventh Circuit, American citizens will routinely be deprived of their privacy rights each time they find themselves at the U.S. border.

130. *See, e.g.*, United States v. Vergara, 884 F.3d 1309, 1317 (11th Cir. 2018) (Pryor, J., dissenting); *Touset*, 890 F.3d at 1236 (requiring reasonable suspicion for forensic device searches at the border would provide special protections for devices that carry digital contraband).

131. Riley v. California, 573 U.S. 373, 375 (2014).

132. Erik Sofe, *What Personal Data Stays on a Phone*?, Consumer Rep. (Mar. 23, 2016), https://www.consumerreports.org/cell-phones-services/what-personal-data-stays-on-your-phone-/.

133. United States v. Kolsuz, 890 F.3d 133, 145 (4th Cir. 2018).

134. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542–43 (2005).