# REQUIRING WHAT'S NOT REQUIRED: CIRCUIT COURTS ARE DISREGARDING SUPREME COURT PRECEDENT AND REVISITING OFFICER INADVERTENCE IN CYBERLAW CASES

*Michelle Zakarin*



## I. INTRODUCTION

As the age of technology has taken this country by surprise and left us with an inability to formally prepare our legal system to incorporate these advances, many courts are forced to adapt by applying pre-technology rules to new technological scenarios. One illustration is the plain view exception to the Fourth

Amendment.[1] Recently, the issue of officer inadvertence at the time of the search, a rule that the United States Supreme Court has specifically stated is not required in plain view inquiries, has been revisited in cyber law cases.[2] It could be said that courts interested in the existence of officer inadvertence, despite its lack of necessity, are properly doing so as a means of analysis for cyber cases to more suitably adjust to the searches of computers and related technology. The Tenth Circuit has knowingly disregarded Supreme Court precedent, and it continues its disagreement with the Fourth Circuit.[3] This perpetuates a circuit split that should be resolved by the Supreme Court. In anticipation of a judicial resolution, this article is written to outline the problem and explain the positions of the circuits that have addressed this issue.

Section II will provide an overview of the Fourth Amendment, focusing on the history of the plain view doctrine and the Supreme Court's examination of officer inadvertence when analyzing plain view search cases. Section III shifts the focus into the modern era of cyber law cases and how those cases involving plain view searches have been analyzed. Particularly, this Section explains and illustrates that various circuit courts of appeal have been explicitly choosing not to follow Supreme Court precedent when analyzing cyber law cases. Section IV examines the Supreme Court's acknowledgement of differences between cases involving technology and cases that do not have a technology component. Section V explains the need for guidance from the Supreme Court to resolve confusion faced by circuit courts deciding cases involving cyber-related searches subject to the plain view doctrine. This article takes the position that the circuit courts that have deviated from prior Supreme Court precedent are consistent with what the Supreme Court would

1. Much has been written about the plain view doctrine. *See, e.g.*, RayMing Chang, *Why the Plain View Doctrine Should Not Apply to Digital Searches*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31 (2017); William Baude & James T. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821 (2016); Andrew Vahid Moshirnia, *Separating Hard Fact From Hard Drive: A Solution for Plain View Doctrine in the Digital Domain*, 23 HARV. J. L. & TECH 609 (2010).

2. *See* Horton v. California, 496 U.S. 128, 141-42 (1990).

3. *See infra* notes 29-54.

likely rule if the issue of officer inadvertence in plain view cyber-related searches arose before the Court today.

## II. AN OVERVIEW OF THE FOURTH AMENDMENT

### a) History of the Plain View Doctrine

The Fourth Amendment of the United States Constitution protects citizens from unlawful searches and seizures.[4] A search is lawful when a warrant is given to law enforcement to search a particular location.[5] One exception to the warrant requirement is the plain view doctrine, where officers happen to view something in their sight—or in their plain view—while in a place they are lawfully permitted.[6] Evidence seized or found in plain view is not considered a new "search" for purposes of the Fourth Amendment.[7] Therefore, the items observed in plain view are allowed to be seized by the officers.[8] The justification for the plain view exception is that "if contraband is left in open view and observed by a police officer from a lawful vantage point, there has been no invasion of a legitimate expectation of privacy and thus no 'search' within the meaning of the Fourth Amendment—or at least no search independent of the initial intrusion that gave the officers their vantage point."[9]

### b) Supreme Court History on Plain View and Officer Inadvertence

In 1971, the Supreme Court decided *Coolidge v. New Hampshire* and, in a plurality opinion, held that the discovery of evidence in plain view must also be inadvertent on the part of the

4. U.S. CONST. amend. IV.

5. *Horton*, 496 U.S. at 133-34 (citing Arizona v. Hicks, 480 U.S. 463, 469 (1985); United States v. Jacobsen, 466 U.S. 109, 113 (1984)). It should be noted that a search is also lawful when consent is given by an occupant to law enforcement to perform a search. *See, e.g.,* Georgia v. Randolph, 547 U.S. 103, 106 (2006) (citing Illinois v. Rodriguez, 497 U.S. 177, 186 (1990); United States v. Matlock, 415 U.S. 164, 170 (1974)).

6. *Horton*, 496 U.S. at 135-36.

7. *Id.*

8. *Id.*

9. Minnesota v. Dickerson, 508 U.S. 366, 375 (1993).

searching officer.[10] The case involved the vicious murder of a fourteen-year-old girl that shocked and frightened a neighborhood.[11] Warrants were issued by the state attorney general, who also led the murder investigation of the defendant, for the defendant's arrest and for the search of defendant's automobile.[12] Pursuant to the warrant, defendant's automobile was seized by police officers and searched on three separate occasions.[13] Evidence collected from a search of the car was used against the defendant at trial.[14] The defendant was convicted and, on appeal, argued the evidence introduced from a search of his car was unlawfully obtained.[15] The Court agreed, ruling in favor of defendant, that the police officers, although claiming the search was in "plain view," did not inadvertently find the evidence since the officers already knew of the car and its location.[16] Thus, the Court in *Coolidge* held that an officer must inadvertently stumble across the incriminating, unrelated evidence.[17]

Nineteen years later, the Supreme Court once again addressed the issue of officer inadvertence and, this time, a majority of the Court held that officer inadvertence is "not a necessary condition" for plain view searches.[18] In *Horton v. California*, a victim was held up and robbed at gunpoint.[19] The robbers used a stun-gun and stole the victim's personal property.[20] The victim recognized one of the robber's distinctive voice and identified the defendant as one of the suspected

10. 403 U.S. 443, 469 (1971).
11. *Id.* at 445.
12. *Id.* at 447.
13. *Id.* at 447-48.
14. *Id.* at 448.
15. *Id.* at 448-49.
16. *Id.* at 471-73.
17. *Id.* at 469. *See also* Joseph R. Davis, *The Plain View Doctrine (Conclusion)*, THE LEGAL DIGEST (Oct. 1979), https://www.ncjrs.gov/pdffiles1/Digitization/63104NCJRS.pdf (stating that because it was a plurality opinion, there was some uncertainty regarding this "inadvertency requirement" and some states refused to follow it).
18. *Horton*, 496 U.S. at 130.
19. *Id.*
20. *Id.*

robbers.[21] The police obtained a warrant to search defendant's house for the stolen property.[22] The officers did not find the stolen property, but they saw two stun guns and clothing identified by the victim.[23] The police claimed this was in "plain view" because they were legally searching the home.[24] The defendant argued that this evidence could not be used against him because it was not discovered inadvertently.[25] The Court in *Horton* reasoned that inadvertence did not further law enforcement interests generally, nor did it further the interests of the Fourth Amendment.[26] The Court stated, "The suggestion that the inadvertence requirement is necessary to prevent the police from conducting general searches, or from converting specific warrants into general warrants, is not persuasive because that interest is already served by the requirements [of a] warrant . . ."[27] Therefore, the Court upheld the conviction and made it clear that inadvertence was not required as part of the plain view doctrine.[28]

## III. CYBER CASES, THE PLAIN VIEW DOCTRINE AND A RETURN TO THE INADVERTENCE REQUIREMENT

### a) Tenth Circuit

Despite the United States Supreme Court's unambiguous position that inadvertence is not required in plain view searches, its application to cyber-related cases has caused a re-emergence of uncertainty. In 1999, the Tenth Circuit faced a plain view question involving a cyber-related search.[29] Specifically, *United States v. Carey* inquired whether an officer's search of computer files was inadvertent.[30] In *Carey*, a warrant was issued to search

21. *Id.*
22. *Id.* at 130-31.
23. *Id.* at 131.
24. *Id.*
25. *Id.*
26. *Id.* at 138-41.
27. *Id.* at 139.
28. *Id.* at 141.
29. United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).
30. *Id.* at 1273-74.

the defendant's computer for information regarding the sale and distribution of drugs.[31] An officer began the search for this particular information and observed multiple files with "jpg" endings that had sexually explicit names.[32] The officer observed images of child pornography after he copied and opened the files .[33] He then copied approximately 244 jpg files from the computer, and many files contained images of child pornography.[34] The Tenth Circuit held that the plain view exception did not apply because:

> [E]ach time [the officer] opened a subsequent jpg file, he expected to find child pornography and not material related to drugs. Armed with this knowledge, he still continued to open every jpg file to confirm his expectations. Under these circumstances, we cannot say the contents of each of those files were *inadvertently* discovered.[35]

The court continued its examination of inadvertence in a footnote, noting that the initial view of the first jpg file was inadvertent and thus fell within the plain view exception and, therefore, the court's holding was limited to the subsequent viewing of the remaining jpg files.[36]

A few years later, the Tenth Circuit again reviewed the plain view doctrine after a computer search.[37] In *United States v. Walser*, a hotel manager responded to the sounding of a smoke alarm in an unoccupied room, and upon entering, the manager discovered drugs.[38] Police obtained a search warrant to search the rented room for evidence of drugs or related to the sale or use of drugs.[39] In the course of the search for drugs, a police officer discovered a computer, began to search it, and discovered adult pornography.[40] At this point, the officer stopped his search and

31. *Id.* at 1270.
32. *Id.*
33. *Id.* at 1271.
34. *Id.*
35. *Id.* at 1273 (emphasis added).
36. *Id.* at 1273 n.4.
37. United States v. Walser, 275 F.3d 981 (10th Cir. 2001).
38. *Id.* at 983.
39. *Id.* at 983-84.
40. *Id.* at 984.

the computer was taken to the investigation office for further review.[41] Days later, the officer continued the search and opened a file that contained a thumbnail image which he believed to be child pornography.[42] He stopped the search and days later obtained a new warrant to search the computer for child pornography, which was ultimately found on the computer.[43] In its decision as to whether the search fell properly within the plain view doctrine, the Tenth Circuit distinguished the present facts from those in *Carey*. Specifically, the court noted the officer stopped the initial search after he inadvertently found the first photograph and obtained a new warrant for child pornography[44] Therefore, the Tenth Circuit again relied on inadvertent behavior of the officer in rendering its decision.[45]

In *United States v. Burgess*, police officers obtained a warrant to search a laptop for evidence of the delivery or sale of illegal drugs after the laptop was found during a traffic stop.[46] Upon searching the laptop for evidence related to drugs, the officer discovered images of child pornography.[47] The officer immediately stopped his search and obtained a new warrant to search the laptop for child sexual exploitation and over 1,000 illicit images were found on the laptop.[48] In determining whether the search was within the scope of the plain view doctrine, the court acknowledged *Carey*'s reliance on inadvertence and distinguished *Carey* from the present case.[49]

More recently, in 2019, the Tenth Circuit again examined a case involving the plain view doctrine in electronic searches and its decision took into account whether the evidence was discovered inadvertently.[50] In *United States v. Loera*, the court

41. *Id.*
42. *Id.* at 984-85.
43. *Id.* at 985.
44. *Id.* at 987.
45. *Id.*
46. U.S. v. Burgess, 576 F.3d 1078, 1082-83 (10th Cir. 2009).
47. *Id.* at 1084.
48. *Id.*
49. *Id.* at 1092 ("As in this case, the officer in *Carey* inadvertently discovered an image of child pornography while searching for electronic evidence of drug activity.").
50. United States v. Loera, 923 F.3d 907, 918 (10th Cir. 2019).

specifically relied on prior Tenth Circuit precedent in *Carey*, *Walser*, and *Burgess* to justify its departure from the Supreme Court's ruling in *Horton*.[51] The most significant part of this decision, as it relates to searches for digital evidence, was in an acknowledgement found in a footnote.[52]

> We acknowledge that in *Horton v. California*, the Supreme Court held that, in physical searches, 'even though inadvertence is a characteristic of most legitimate plain view searches, it is not a necessary condition.' However, because *Carey*, *Walser*, and *Burgess*, each of which succeeded *Horton* in time, considered the subjective intentions of the searching officers where that information was available, we continue to include inadvertence as a factor to consider when deciding whether an electronic search fell within the scope of its authorizing warrant or outside of it. The fundamental differences between electronic searches and physical searches, including the fact that the electronic search warrants are less likely prospectively to restrict the scope of the search, justify our inclusion of that factor.[53]

Thus, the court recognized that its reasoning on this subject was inconsistent with Supreme Court precedent, but continued to follow this departure nonetheless.[54]

b) Other Circuits

In 2010, the Sixth Circuit faced the issue of whether an officer's search of a laptop computer was proper after consent was given to search for drugs and related paraphernalia.[55] The court relied on rulings from the Tenth Circuit.[56] In doing so, the court paid close attention to the fact that the officer in the case, like the officer in *Walser*, "stumbled upon" the initial electronic file.[57] Thus, the inadvertence of the officer was a deciding factor in the

51. *Id.* at 919-20.
52. *Id.* at 919 n.3.
53. *Id.*
54. *Id.*
55. United States v. Lucas, 640 F.3d 168, 171-72 (6th Cir. 2010).
56. *Id.* at 179.
57. *Id.*

court's ultimate determination.[58]

In *United States v. Mann*, the defendant secretly installed a camera in the women's locker room to capture images of women as they undressed at his work as a lifeguard instructor for the Red Cross.[59] A woman in the locker room noticed the camera and played the video, which revealed the defendant himself installing the camera.[60] The camera and its footage were turned over to the police department.[61] A search warrant was issued for the defendant's home to look for more images of women in locker rooms.[62] Officers then discovered images of child pornography after defendant's computer was searched.[63] The Seventh Circuit held the search was proper because through the course of searching for images of adult women, the officer "stumbled upon" the child pornography images.[64] The Tenth Circuit's use of the term "inadvertent" in *Carey* guided the court's reasoning.[65]

With respect to inadvertence, the Ninth Circuit distinguished its facts in *United States v. Giberson* from those in *Carey*.[66] In *Giberson*, the court explicitly noted that a search pursuant to a warrant for fake identification documents was proper because the officer inadvertently discovered child pornography during the search.[67] In *United States v. Whaley*, the Eleventh Circuit considered whether a search via consent from the defendant exceeded its scope.[68] The defendant consented to have a flight simulator video located on his laptop viewed by an officer.[69] When the officer tried to display the flight simulator, he clicked the icon of a different video containing child pornography.[70] The defendant argued that the search was improper because it

58. *Id.*
59. 592 F.3d 779, 780 (7th Cir. 2010).
60. *Id.*
61. *Id.*
62. *Id.* at 780-81.
63. *Id.* at 781.
64. *Id.* at 783.
65. *Id.* at 784 (citing *Carey*, 172 F.3d at 1273).
66. 527 F.3d 882, 890 (9th Cir. 2009) (citing *Carey*, 172 F.3d at 1273).
67. *Id.*
68. 415 Fed. Appx. 129 (11th Cir. 2011).
69. *Id.* at 131.
70. *Id.*

exceeded the scope of his consent.[71] The court held this discovery was within the scope of the search of the laptop because the officer discovered the video inadvertently.[72] To support this determination, the court examined cases from other circuits, including *Walser*, *Mann*, and *Burgess*, and particularly noted each court's reliance on inadvertence.[73] Additionally, a number of district courts[74] and one state court[75] have also required officer inadvertence in issues involving cyber searches.

c) Some Uncertainty and Confusion

In *United States v. Williams*, the Fourth Circuit examined a case involving a search of computers and other electronic storage devices where the officer ultimately discovered child pornography.[76] The defendant argued the search both violated his Fourth Amendment right and was inconsistent with the Tenth Circuits ruling in *Carey*, because the officer's discovery of the evidence in question was not inadvertent.[77] The Fourth Circuit was unpersuaded by *Carey*'s ruling on inadvertence, however, and instead relied on the Supreme Court's ruling in *Horton*, which found that inadvertence is not required in a plain view search.[78] The court explained, "We conclude that even though inadvertence is a characteristic of most legitimate 'plain-view' seizures, it is not a necessary condition. To the extent that

71. *Id.* at 130.

72. *Id.* at 134.

73. *Id.* (citing *Mann*, 592 F.3d at 782-86; *Burgess*, 576 F.3d at 1092-95; *Walser*, 275 F.3d at 983-85).

74. United States v. Kim, 677 F. Supp. 2d 930, 944 (S.D. Tx. 2009) (The court upheld the validity of a cyber search, relying on *Carey* and *Giberson*, both of which relied specifically on the inadvertent discovery of evidence. Interestingly, the court began its analysis noting that inadvertence is "not required" under *Horton*, it went on to follow cases that relied on inadvertence.); United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (The court noted that the *Carey* court's reasoning about inadvertence discovery was applicable to this case as well.).

75. Frasier v. State, 794 N.E.2d 449, 466 (Ind. Ct. App. 2003) (holding that files were in plain view because the image files were inadvertently discovered).

76. 592 F.3d 511, 516 (4th Cir. 2010).

77. *Id.* at 523.

78. *Id.* at 522-23 (citing *Horton*, 496 U.S. at 130).

these cases suggested that inadvertence is a requirement of a warrantless plain-view seizure, they are now overruled by *Horton*."[79]

This explicit rejection demonstrates a circuit split. Currently, the Fourth Circuit stands alone in its adherence to *Horton* when applying inadvertence to cyber law cases.[80] As a result, potential confusion exists for circuits that have yet to address this issue. In effect, the question becomes whether a circuit should adhere to the Supreme Court's ruling in *Horton* or, instead, follow other circuits that have carved out a special rule where inadvertence is required for plain view searches in cyber-related cases.

## IV. THE SUPREME COURT AND ITS VIEW OF CASES INVOLVING TECHNOLOGY

Guidance as to whether the Supreme Court, in the context of cyber law cases, will continue to rely on *Horton* or utilize the analyses followed by the Tenth Circuit and other circuit courts, can be gleaned from the Court's treatment in other cyber-related cases. In *Kyllo v. United States*, the Supreme Court faced a question about whether the government's use of thermal image sensing technology was a search within the meaning of the fourth amendment.[81] Police used thermal image devices to scan the heat emanating from defendant's house, based on a suspicion that marijuana was being grown inside the home using heat lamps.[82] The device showed certain parts of the home were substantially warmer than other nearby residences.[83] Based on this information, a magistrate issued a warrant to search for marijuana at defendant's home.[84] Thereafter, marijuana was found in defendant's home, and defendant was subsequently charged with violations of federal drug laws.[85] The Court held the

79. *Id.* at 523 n.3.

80. *Id.* (This is the opposite conclusion reached by the Tenth Circuit in *Loera*, where the court remarkably acknowledged *Horton* but declined to follow the holding.)

81. 533 U.S. 27, 29 (2001).

82. *Id.* at 29-30.

83. *Id.* at 30.

84. *Id.*

85. *Id.*

use of the thermal imaging technology was itself a search, and therefore, a warrant was needed in order to use it for this purpose.[86] Otherwise, the Court noted, it would leave homeowners "at the mercy of advancing technology."[87]

In 2014, the Supreme Court decided *Riley v. California* and ruled on whether a search incident to arrest was properly made.[88] In *Riley*, the search was of a cell phone incident to a lawful arrest.[89] The Court held that searches of digital data are different from other types of searches and cannot be searched incident to arrest without a warrant.[90] Specifically, the Court stated that the term "cell phone" can be misleading because usually these phones are actually minicomputers and, therefore, they are different from any other object found on an arrestee's person.[91] In its reasoning, the Court stated "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person . . . [o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity."[92] While this case did not analyze the plain view exception, its broad acknowledgement that a difference exists between searches of computers and other forms of searches lends itself to similar reasoning when the search is indeed within the context of the plain view exception. While *Horton* remains controlling law today, the context of its decision in 1990 merits consideration of the fact that computers or cell phones were not nearly as prevalent as they are today.

In 2018, the Supreme Court again recognized the differences between physical searches and searches of data in electronic devices.[93] In *Carpenter v. United States*, the police acquired defendant's cellular location points spanning a period of over 127 days after a magistrate judge ordered the cellular companies to

86. *Id.* at 40.
87. *Id.* at 35.
88. Riley v. California, 573 U.S. 373, 382, 134 S. Ct. 2473, 2482 (2014).
89. *Id.* at 378-79, 134 S. Ct. at 2480.
90. *Id.* at 386, 403, 134 S. Ct. at 2485, 2495.
91. *Id.* at 393, 134 S. Ct. at 2489.
92. *Id.*
93. Carpenter v. United States, 138 S. Ct. 2206, 2214, 201 L. Ed. 2d 507, 517-19 (2018).

release this information.[94] As a result, the defendant was subsequently charged with robbery.[95] Because access to this information provided the government with extremely accurate surveillance data, the Court held that a warrant was necessary to properly obtain cell phone location information.[96] In refusing to allow the government unrestricted access to this type of digital information, the Court expressly noted that changes in technology need to be analyzed carefully by this Court so that protections remain intact.[97]

Notably, the Supreme Court has expressed time and again its understanding of the way technology brings new, unanticipated legal challenges. Many of these challenges cannot be easily resolved through the use of traditional legal principles. Thus, courts are grappling with finding equitable results, even if that means straying from existing precedent. While the end result may appear fair and just, the process should be more streamlined to provide clear guidance to courts facing similar issues. As such, it is increasingly necessary for the Supreme Court to take action and rule specifically with respect to the issue of whether inadvertence should be required under the plain view doctrine within the context of cyber-related searches, where a decision by the highest court in the land stands as the most streamlined guidance possible.

## V. THE SUPREME COURT NEEDS TO REVISIT *HORTON* AND MODIFY ITS HOLDING TO REQUIRE INADVERTENCE IN DIGITAL SEARCH CASES

With respect to resolving this circuit split, one view may be to charge Congress with proposing legislation to provide a framework on handling cyber-relates searches. While legislative clarification may work, a decision by the Supreme Court providing guidance on this specific issue remains a more suitable solution. A review of Supreme Court precedent suggests that

94. *Id.* at 2212, 201 L. Ed. 2d. at 516.

95. *Id.*

96. *Id.* at 2221, 201 L. Ed. 2d. at 525 (Note that the Court cited to *Kyllo* and *Riley* in this decision).

97. *Id.* at 2223, 201 L. Ed. 2d. at 528.

when faced with cases involving technology, the Court is willing and able to address these concerns without the need for congressional action. The Court has explicitly noted that searches of computers are different from other searches; the storage capacity is practically endless and the ability to uncover something incriminating is possible.[98] Although not required under current Supreme Court jurisprudence, courts requiring officer inadvertence for digital searches are properly protecting citizens from the possibility of obtaining a warrant for one thing, like evidence of drugs, when officers are looking for another. As the Supreme Court has stated, "inadvertence is a characteristic of most legitimate 'plain-view' seizures."[99] Digital searches, where the mere click of a mouse may reveal an excessive amount of information, make it more difficult to adhere to this standard without courts returning to an examination of inadvertence.

It may be years before the Supreme Court revisits whether inadvertence is required in digital searches. The majority of circuits and federal district courts addressing this issue neither follow nor mention *Horton*'s holding. In fact, only one circuit is explicitly following *Horton*'s holding when examining a cyber-related search case.[100] To provide authority and guidance to law enforcement agencies and courts, however, the Supreme Court needs to revisit the plain view doctrine within the context of cyber cases. Only then will the Court have the opportunity and ability to decide whether inadvertence is not required in all searches of evidence, or whether a modification is needed to require inadvertence within the context of digital searches.

98. *See, e.g., Riley*, at 393, 134 S. Ct. at 2489.
99. *Horton*, 496 U.S. at 130.
100. *See* United States v. Williams, 592 F.3d 511 (4th Cir. 2010).