GIR Global Investigations Review

Americas Investigations Review

2025

US courts zero in on border searches of electronic devices

Americas Investigations Review

2025

The Americas Investigations Review contains insight and thought leadership from pre-eminent practitioners from the region. Part retrospective, part primer, part crystal ball – and 100 per cent essential reading – here you can read about some of the most important developments affecting international investigations in North and Latin America, supported throughout with footnotes and relevant statistics.

Generated: August 17, 2024

GIR Global Investigations Review

Explore on GIR

US courts zero in on border searches of electronic devices

Joel M Cohen, Maria Beguiristain, Marietou Diouf and Robert J DeNault
White & Case LLP

Summary

IN SUMMARY
DISCUSSION POINTS
REFERENCES IN THIS ARTICLE
RILEY V CALIFORNIA
CARPENTER V UNITED STATES
US CIRCUIT SPLIT ON CELL PHONE BORDER SEARCHES
CONCLUSION: PATH TO THE SUPREME COURT

IN SUMMARY

In this article, we will discuss the US government's authority to search electronic devices, particularly cell phones, in reliance on the border search exception to the Fourth Amendment. First, we review the border search exception, which allows searches at the border without a search warrant, probable cause or reasonable suspicion. Next, we examine recent Supreme Court cases that restrained the government's ability to access cell phone data without a search warrant. Finally, we analyse how different jurisdictions around the United States are applying the cases' rationale to cell phone searches in the border context and limiting the government's ability to search electronic data at the border without a search warrant, probable cause or reasonable suspicion.

DISCUSSION POINTS

- US law enforcement enjoys wide latitude to conduct searches at the border without a warrant, probable cause or reasonable suspicion
- Some courts have started to narrow the ability of law enforcement to forensically search cell phones as part of a border search, citing recent US Supreme Court cases recognising the unique sensitivity of cell phone evidence
- In 2023, two judges in New York held that law enforcement must obtain a search warrant to search cell phones forensically or manually
- In appropriate jurisdictions, counsel should consider arguing for suppression of evidence collected from a cell phone during a border stop or for the return or destruction of unlawfully seized data under Federal Rule of Criminal Procedure 41(g)

REFERENCES IN THIS ARTICLE

- *Riley v California*
- *Carpenter v United States*
- *United States v Kolsuz*
- *United States v Touset*
- *United States v Cano*
- *United States v Shuren Qin*
- *United States v Xiang*
- *United States v Smith*
- *United States v Alisigwe*

Under the Fourth Amendment to the US Constitution, law enforcement stops typically must be supported by reasonable suspicion of wrongdoing,[1] while searches, absent delineated exceptions, typically must be accompanied by a search warrant supported by probable cause.[2] However, under a doctrine known as the border search exception, when a person is travelling across a US border, these requirements generally are waived, and law enforcement may conduct stops and searches regardless of whether or not there is reasonable suspicion

or a warrant.[3] Recently, border and other law enforcement agents have pushed this exception to new limits by relying on it to – without a search warrant or reasonable suspicion – seize, search and even image and copy data on cell phones and computer hard drives carried by travellers.

Historically, the border search exception has been grounded in the government's interest – long held to be at its zenith at an international border[4] – in preventing the entry of contraband or persons who may bring harm into the United States.[5] Under the exception, the government may conduct routine searches without any suspicion of wrongdoing by a traveller.[6] For non-routine seizures – defined by courts as 'exceptionally invasive' searches – courts require reasonable suspicion (eg, some suspicion of individual wrongdoing).[7]

To determine whether a search is sufficiently invasive to qualify as non-routine, courts typically focus on how deeply it intrudes into a person's privacy.[8] For example, searches of outer clothing, luggage, a purse or a wallet are considered routine because they are not particularly invasive.[9] On the other hand, strip searches are considered sufficiently invasive to be nonroutine.[10]

Predictably, travellers are often stopped while carrying cell phones, laptops or other electronic devices, and law enforcement agents sometimes seek to search the contents of those devices as part of a border search. In both 2022 and 2023, there were over 40,000 border searches of electronic devices, a nearly 25 per cent jump since 2018.[11] And that increase indicates a trend: in the first half of financial year 2024, there have been over 22,000 electronic device searches at the border.[12]

Importantly, there are two kinds of electronic device searches that occur at the border: manual searches (where the agent scrolls through immediately available material on a device) and advanced searches (where the agent seizes a device, forensically images it and retains the forensic image for review). In a string of recent cases, federal district and circuit courts have considered arguments that manual or advanced searches of devices require search warrants, probable cause or reasonable suspicion. Courts wrestling with this issue have taken note of two notable Supreme Court decisions that rejected government arguments that law enforcement has a right to obtain cell phone data without a search warrant under different exceptions to the Fourth Amendment.

RILEY V CALIFORNIA

In Riley v California,[13] the Supreme Court addressed whether cell phone searches that occur 'incident to lawful arrest' are exempted from the warrant requirement, like similar searches of an individual's person, vehicle or other objects they have on their person at the time of arrest.[14] At the outset, Chief Justice Roberts, writing for the Court, stressed that cell phones have remarkable characteristics such that precise guidance from the founding era is not available.[15] He framed the task before them as weighing the degree to which warrantless search of a cell phone intrudes upon an individual's privacy against the degree to which it is needed for the promotion of government interests under the lawful arrest exception.[16]

The Court concluded that the privacy intrusion resulting from a cell phone search is so great that it cannot be done without a search warrant, even incident to a lawful arrest.[17] Rejecting the argument that cell phones are like other objects kept on an arrestee's person, the Court noted that '[c]ell phones differ in both a quantitative and qualitative sense' since 'many [cell phones] are in fact minicomputers that also happen to have the capacity to be used as a telephone'.[18] Chief Justice Roberts rejected arguments that officers could

limit warrantless searches to 'areas of the phone where an officer reasonably believes that information relevant to the crime' exists because officers would not be able to discern in advance what information would be found where and such standards would 'launch courts on difficult line-drawing expedition[s]'.[19]

The Court concluded Riley by noting that while its holding may prevent law enforcement from examining key evidence, '[p]rivacy comes at a cost', and law enforcement remains free to obtain a warrant to review cell phone evidence.[20] Further, the Court noted that the 'exigent circumstances exception' – which permits law enforcement to conduct warrantless searches in certain scenarios, such as emergencies – still would permit warrantless searches of cell phones in extreme circumstances.[21]

CARPENTER V UNITED STATES

Four years later, the Supreme Court decided another Fourth Amendment case about cell phone data, United States v Carpenter.[22] In Carpenter, the Court addressed whether the Fourth Amendment applies to a person's cell phone records, including cell site location data, which could be obtained from wireless carriers by prosecutors at that time under the Stored Communications Act if prosecutors had 'reasonable grounds' for believing they were relevant to an ongoing investigation.[23]

The government argued that the 'third-party doctrine' – a doctrine that excludes business records created and maintained by third parties from most individual Fourth Amendment protections – also excluded cell site location data from Fourth Amendment protection.[24] The Court disagreed. According to Chief Justice Roberts (again writing for the Court) the government's argument 'fail[ed] to contend with the seismic shifts in digital technology'.[25] The Court described wireless carriers as 'not your typical witnesses', with a memory that is 'nearly infallible' and data that qualified as an 'exhaustive chronicle of location information'.-[26] The Court not only determined that collection of location data from carriers qualifies as a search under the Fourth Amendment but also held that the government 'must generally obtain a warrant supported by probable cause before acquiring such records'.[27]

Describing the reasonable grounds showing under the Stored Communications Act as 'fall[ing] well short of the probable cause required for a warrant', the Court described cell site location information as an 'entirely different species of business record' and cautioned that the Court 'has been careful not to uncritically extend existing precedents' when 'confronting new concerns wrought by digital technology'.[28] In short, Carpenter instructs that when seeking a subscriber's location information from a carrier, 'the Government's obligation is a familiar one—get a warrant'.[29] Once again, the Court caveated that the exigent circumstances exception would permit warrantless access to cell site location information in appropriate situations.[30]

While Carpenter involves efforts to collect cell phone evidence from third parties, not individuals, the concerns that underpin the Court's reasoning in both cases suggest the Court views warrantless searches of cell phones in reliance on exceptions to the Fourth Amendment as unlawful intrusions of privacy. The Court has not yet applied this line of cases to the border search exception, but district and circuit courts around the United States frequently cite to Riley and Carpenter as they consider whether cell phone searches at the border should be subject to some Fourth Amendment protections or a search warrant requirement.

US CIRCUIT SPLIT ON CELL PHONE BORDER SEARCHES

Courts grappling with the border search problem confront two separate issues. First, there is a dispute over whether reasonable suspicion is required to justify a search of a cell phone. It appears that all federal circuit courts that have confronted the issue (but not all district courts)[31] currently agree that manual searches – opening the phone and browsing its immediately available contents – are permissible under the border search exception and do not require any suspicion, reasonable or otherwise. But advanced, or forensic searches – detaining devices for forensic imaging, copying and prolonged review – are where courts diverge.

Three circuit courts of appeal – the First, Fourth and Ninth – have concluded that advanced searches of a cell phone or electronic device are non-routine and require reasonable suspicion.[32] But the Eleventh Circuit has concluded exactly the opposite and held that cell phones searches, whether manual or advanced, are routine searches that can be conducted without reasonable suspicion.[33] Other circuit courts of appeal have not yet fashioned formal standards, but some have started to – or acknowledged a need to – do so in dicta referencing Riley, Carpenter and the current circuit split.[34] Functionally, in certain jurisdictions the government now is seeking search warrants to conduct forensic searches instead of simply resting on its border search authority, cutting against arguments that the government enjoys clear authority under the law to seize and search cell phones pursuant to the border search exception.

Notably, in federal circuits where no firm rule is set, district courts are setting more restrictive and specific standards. For example, in autumn 2023, a court in the Southern District of New York became the first court in the country to conclude that law enforcement always needs a search warrant to conduct a cell phone search during a border stop if the search involves copying and searching the phone.[35] A few months later, a different Southern District of New York court held that even manual searches of cell phones must be supported by reasonable suspicion.[36] Prior to that, a DC district court applied Riley to searches of electronic devices at the border and found that the imaging and search of the entire contents of a laptop, aided by forensic software, for a period of unlimited duration and an examination of unlimited scope, were so invasive of privacy and disconnected from the government interests under the border search exception that they were patently unreasonable under the Fourth Amendment.[37] Separately, courts also have confronted the issue of whether an individual may be forced to disclose biometric passcodes for devices seized during a border search and have addressed whether the refusal to provide passwords permits the government to use reasonable time to attempt brute force entry of seized devices.[38]

Practitioners in circuits where reasonable suspicion is required to conduct an advanced search as a result of a border stop should consider moving to exclude evidence derived from the forensic imaging or prolonged search of a device if there is support for the argument that there was not reasonable suspicion to support such a search. In cases where the government rests on its border search authority and reasonable suspicion may exist, practitioners should consider arguing that the government should have been required to establish probable cause and should have obtained a search warrant. Similarly, in jurisdictions with no clear rule on this issue, practitioners should consider moving to exclude evidence derived from an advanced search of a device without any search warrant on the grounds that such a search violates the Fourth Amendment. In circuits that have explicitly required reasonable suspicion to conduct an advanced search, practitioners also should consider actions under Federal Rule of Criminal Procedure 41(g) to demand return

or destruction of unlawfully seized property if there is factual support for a claim that border agents seized and copied a device without any reasonable suspicion to do so.

Secondary Split On The Scope Of An Advanced Search

Even among the circuits concluding reasonable suspicion is required for advanced searches, courts have fashioned varying parameters on the appropriate scope of a search. For example, the First Circuit has defined advanced forensic searches as 'non-routine' and limits them to evidence of contraband or evidence of activity in violation of the laws enforced or administered by US Customs and Border Protection (CBP) or Immigration and Customs Enforcement (ICE).[39] The Fourth Circuit limits advanced searches to evidence connected to reasonable suspicion of an ongoing border-related crime.[40] In the Ninth Circuit, advanced searches must be limited to evidence of digital contraband (ie, data that is itself illegal to possess, such as child sexual abuse material, stolen data or classified information).[41]

The table below summarises the current jurisprudence rules in different federal circuits addressing the topic.

Table 1: Current jurisprudence rules in different federal circuits

Circuit	Reasonable suspicion required for advanced search	Limitations on scope of search	Limits
First	Yes	Yes	Border - related crime
Second	No rule	No rule	No rule
Third	No rule	No rule	No rule
Fourth	Yes	Yes	Ongoing border - related crime
Fifth	No rule	No rule	No rule
Sixth	No rule	No rule	No rule
Seventh	No rule	No rule	No rule
Eighth	No	No	N/A
Ninth	Yes	Yes	Solely digital contraband
Tenth	No rule	No rule	No rule
Eleventh	No	No	N/A
DC	No rule	No rule	No rule

Overall, in appropriate circumstances, practitioners in the First, Fourth and Ninth Circuits should consider moving to exclude evidence premised on arguments that a search exceeded the bounds of the border search exception if the government obtained evidence of crimes that were not border-related crimes within the jurisdiction of CBP or ICE or searched areas

of electronic devices in areas in which digital contraband (ie, a sexually explicit photograph of a minor) is unlikely to be found.

CONCLUSION: PATH TO THE SUPREME COURT

Given the lack of uniformity in the approaches employed by district and circuit courts around the country regarding this issue, and the Supreme Court's recent decisions in Riley and Carpenter, it seems likely the Court soon may address whether border searches of cell phones come within the ambit of the border search exception to the Fourth Amendment. Reading Riley closely suggests the Court will focus on two particular areas of interest. First, it may focus on the routine versus non-routine analysis to find that cell phone searches are not routine as a general matter because the invasiveness of the search far outweighs the government's interests in a border search. Second, some of the dicta in the Court's final paragraphs in Riley suggests the Court may disagree with circuits that have endorsed the use of special parameters around an advanced search.

The Riley Court specifically rejected arguments that officers could limit searches to areas of a phone where an officer reasonably believes information relevant to a crime exists because officers cannot discern in advance what information would be found where.[42] The Court went on to reject several other proposed standards because they would 'launch courts on difficult line-drawing expedition[s]'.[43] And the Court also has made clear that the purpose underlying the border search exception is not limited to interdicting contraband; rather, it serves to protect against 'anything harmful' coming in to the United States, including communicable diseases, narcotics or explosives.[44] This may suggest that rules imposed in the First, Fourth and Ninth Circuit that limit searches to 'border-related crimes' or 'digital contraband' are unworkable standards.

While it remains unclear how the Supreme Court may limit border searches of cell phones or other electronic devices, the rationales in Riley and Carpenter and emerging trends in district and circuit courts around the country strongly suggest the Court likely will impose some limits on the government's ability to seize, copy and review expansive repositories of data taken from travellers under the border search exception to the Fourth Amendment.

Endnotes

[1] Ashcroft v al-Kidd, 563 U.S. 731, 749 n.3 (2011) (Ginsburg J, concurring).

[2] Riley v California, 573 U.S. 373, 403 (2014); see also Arizona v Gant, 556 U.S. 332, 338 (2009).

[3] United States v Ramsey, 431 U.S. 606, 616 (1997).

[4] United States v Flores-Montano, 541 U.S. 149, 152 (2004).

[5] SeeUnited States v Kolsuz, 890 F.3d 133, 137 (4th Cir. 2018) (citing United States v Montoya de Hernandez, 473 U.S. 531, 538 (1985)).

[6] 'Reasonable suspicion' is not explicitly defined in this context but generally has been interpreted to mean 'suspicion . . . that the person has engaged in wrongdoing'. al-Kidd, 563 U.S. at 749 n.3.

[7] United States v Montoya De Hernandez, 473 U.S. 531, 541 (1985) (holding the detention of a traveller at the border was beyond the scope of a routine customs search and inspection

was justified if agents, considering all the facts, reasonably suspect that the traveler was smuggling contraband).

[8] Kolsuz, 890 F.3d at 144; see also United States v Irving, 452 F.3d 110, 123 (2d Cir. 2006) ('[T]he level of intrusion into a person's privacy is what determines whether a border search is routine.')

[9] SeeIrving, 452 F.3d at 123 (citing United States v Asbury, 586 F.2d 973, 975-76 (2d Cir. 1978).

[10] Montoya De Hernandez, 473 U.S. 531, 541.

[11] https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics.

[12] id.

[13] Riley v California, 573 U.S. 373 (2014).

[14] SeeWeeks v United States, 232 U.S. 383 (affirming the government's right to search the person of a legally arrested individual to discover and seize fruits or evidence of crime).

[15] Riley, 573 U.S. at 385 (describing cell phones as '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').

[16] Seeid. (citing Wyoming v Houghton, 526 U.S. 295, 300 (1999)).

[17] Riley, 573 U.S. at 386.

[18] id. at 391.

[19] id. at 401.

[20] id.

[21] id. at 402.

[22] Carpenter v United States, 585 U.S. 296 (2018).

[23] id. at 301-2.

[24] id. at 313.

[25] id.

[26] id. at 314.

[27] Carpenter, 585 U.S. at 316.

[28] id. at 317.

[29] id.

[30] id. at 319-20.

[31] See infra n. 34.

[32] United States v Shuren Qin, 57 F.4th 343, 346-47 (1st Cir. 2023); see alsoAlasaad v Mayorkas, 988 F.3d 8, 21 (1st Cir. 2021); United States v Cano, 934 F.3d 1002, 1016 (9th Cir. 2019) (holding reasonable suspicion is required for a forensic search);United States v Kolsuz, 890 F.3d 133, 137 (4th Cir. 2018).

[33] United States v Touset, 890 F.3d 1227, 1235 (11th Cir. 2018).

[34] See, eg,United States v Castillo, 70 F.4th 894, 898 (5th Cir. 2023) (citing Rileyand the circuit split regarding whether reasonable suspicion is required to conduct forensic searches of cell phones under border search exception);United States v Xiang, 67 F.4th 895, 900-01 (8th Cir. 2023) (citing Riley and noting circuit split, but deciding case at hand did not require adoption of a reasonable suspicion standard for forensic searches); see alsoUnited States v Alisigwe, 2023 U.S. Dist. LEXIS 213415, at *10-12 (S.D.N.Y. 30 November 2023) (noting that neither the Supreme Court nor the Second Circuit has had occasion to decide whether cellphone searches at the border are routine, non-routine, or sui generis and holding cell phone searches 'cannot be conducted without reasonable suspicion of criminal activity because they are not border searches . . . [as] even a manual review of the contents of a person's cellphone is on the "more invasive" end of the search spectrum.'); United States v Kamaldoss, 2022 U.S. Dist. LEXIS 73897, at *34 n.10 (S.D.N.Y. 22 April 2022) (citing Kolsuz and noting that while the Second Circuit has not spoken to the scope of forensic searches at the border, 'as a general rule, the scope of a warrant exception should be defined by its justifications' and that other circuits have limited warrantless border searches to individualized suspicion of offences that bear some nexus to the border search exception's goal of protecting national security, collecting duties, blocking entry of unwanted persons or disrupting efforts to smuggle contraband).

[35] United States v Smith, 673 F. Supp. 3d 381, 390-94 (S.D.N.Y. 2023) (holding that the government must obtain a warrant to copy and search an American citizen's cell phone absent exigent circumstances after finding that 'none of the rationales supporting the border search exception justifies applying it to searches of digital information contained on a traveler's cell phone, and the magnitude of the privacy invasion caused by such searches dwarfs that historically posed by border searches and would allow the Government to extend its border search authority well beyond the border itself'); but seeUnited States v Gavino, No. 22-CR-136 (RPK), 2024 WL 85072, at *6 (E.D.N.Y. 7 January 2024) (finding Smith's reasoning unpersuasive as 'searches of electronic devices at the border have value not just in detecting contraband itself on a device but in determining whether a traveler is carrying drugs or other dangerous or illegal items, as well as whether a traveler ought not to be admitted for national security, immigration or other reasons').

[36] United States v Alisigwe, 2023 U.S. Dist. LEXIS 213415, at *12 (S.D.N.Y. 30 November 2023).

[37] United States v Jae Shik Kim, 103 F. Supp. 3d 32, 56-59 (D.D.C. 2015).

[38] See, eg, Matter of Residence in Oakland, Ca., 354 F. Supp. 3d 1010, 1014-15 (N.D. Cal. 2019).

[39] Shuren Qin, 57 F.4th at 346-47; see also Alasaad, 988 F.3d at 21.

[40] Kolsuz, 890 F. 3d at 143.

[41] Cano, 934 F.3d at 1016.

[42] Riley,573 U.S. 373, 399.

[43] id.

[44] United States v Montoya de Hernandez, 473 U.S. 531, 544 (1985).

WHITE & CASE

Joel M Cohen joel.cohen@whitecase.com
Maria Beguiristain mbeguiristain@whitecase.com
Marietou Diouf marietou.diouf@whitecase.com
Robert J DeNault robert.denault@whitecase.com

3000 El Camino Real , 2 Palo Alto Square, Suite 900, Palo Alto CA 94306, United States

Tel: +1 650 213 0355

https://www.whitecase.com