
CRIMINAL PROCEDURE — FOURTH AMENDMENT — NINTH CIRCUIT LIMITS THE SCOPE OF WARRANTLESS CELL PHONE SEARCHES AT THE BORDER. — *United States v. Cano*, 934 F.3d 1002 (9th Cir. 2019).

Each year, border officials examine tens of thousands of electronic devices as they cross into and out of the United States.¹ Although these devices contain staggering amounts of private data,² the Fourth Amendment affords their owners far less protection than they might imagine³ due to an exception to the warrant requirement that gives government officials broad authority to conduct warrantless searches at the United States' international border.⁴ And though many courts have emphasized that there must be *some* limit on this “border search exception,”⁵ the circuit courts have sharply divided over the nature of any such limit.⁶ Recently, in *United States v. Cano*,⁷ the Ninth Circuit held that the border search exception authorized warrantless cell phone searches only when directed at finding digital contraband.⁸ Though on its face *Cano* increased Fourth Amendment protections for border crossers,⁹ the court's permissive application of its newly announced standard

¹ Laura K. Donohue, *Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 YALE L.J.F. 961, 961–62 (2019).

² *Id.* at 1010 (noting that a cell phone search exposes “the traveler's entire life, as well as significant amounts of others' private affairs”).

³ See Matthew B. Kugler, Comment, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1195 (2014) (finding that, for most types of electronic border searches, less than eleven percent of surveyed Americans believed the searches could be conducted without some articulable suspicion).

⁴ The exception to the Fourth Amendment's warrant requirement is premised on the “longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into [the United States].” *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

⁵ See, e.g., *United States v. Alfaro-Moncada*, 607 F.3d 720, 729 (11th Cir. 2010) (noting that “[e]ven at the border . . . reasonable suspicion is required for highly intrusive searches”); *United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008) (en banc) (declining to hold that “at the border, anything goes”); *United States v. De Gutierrez*, 667 F.2d 16, 19 (5th Cir. 1982) (holding that reasonable suspicion is required for a strip search by a customs agent).

⁶ See Note, *The Border Search Muddle*, 132 HARV. L. REV. 2278, 2284–85 (2019) (describing the Fourth Circuit's position in *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018), on one hand, and the Eleventh Circuit's position in *United States v. Touse*, 890 F.3d 1227 (11th Cir. 2018), on the other, as “representative of the battle lines,” Note, *supra*, at 2284).

⁷ 934 F.3d 1002 (9th Cir. 2019).

⁸ *Id.* at 1007.

⁹ See, e.g., Maura Dolan, *Ruling Limits Border Agents' Ability to Search Cellphones*, L.A. TIMES (Aug. 16, 2019, 3:24 PM), <https://www.latimes.com/california/story/2019-08-16/9th-circuit-illegal-cellphone-search-border-agents> [<https://perma.cc/2PAF-ECYK>]; Sophia Cope & Adam Schwartz, *Ninth Circuit Goes a Step Further to Protect Privacy in Border Device Searches*, ELECTRONIC FRONTIER FOUND. (Aug. 22, 2019), <https://www EFF.org/deeplinks/2019/08/ninth-circuit-goes-step-further-protect-privacy-border-device-searches> [<https://perma.cc/XE46-VEC3>]; Tim Cushing, *Ninth Circuit Says Warrantless Device Searches at the Border Must Be Limited to Searches for Contraband*, TECHDIRT (Aug. 27, 2019, 3:14 AM), <https://www.techdirt.com/>

on the scope of the border search exception demonstrates the illusory nature of these purported protections.

On July 25, 2016, Miguel Cano attempted to cross from Mexico into the United States at the San Ysidro Port of Entry.¹⁰ Customs and Border Protection officers referred Cano to a secondary inspection, which revealed more than thirty pounds of cocaine sealed inside his spare tire.¹¹ The officers arrested Cano.¹² While Cano was in custody, Homeland Security Investigations (HSI) agents conducted three searches of his cell phone.¹³ The agents conducted the first and second searches manually, examining Cano's text messages and call log, and recording some of the listed phone numbers.¹⁴ During the third search, the agents used Cellebrite software to download data from Cano's phone.¹⁵

Before trial, Cano moved to suppress the evidence obtained from the searches, arguing that the HSI agents violated his Fourth Amendment rights by searching his phone without a warrant.¹⁶ The district court held that the agents were entitled to conduct the searches under the border search exception.¹⁷ The court rejected Cano's argument that the exception applied only where the purpose of the search was to "prevent[] the entry of unwanted persons or things,"¹⁸ determining that "border search cases do not turn on the purpose or motivation behind the search."¹⁹ Instead, the court analyzed the searches exclusively under the two-tiered suspicion framework of *United States v. Cotterman*,²⁰ which required reasonable suspicion for "forensic" searches, and no suspicion for "manual" searches.²¹ A forensic search is distinguished from a standard "manual" search by its "comprehensive and intrusive nature" and use of "computer forensic software."²² The court found even the most

articles/20190816/20021742803/ninth-circuit-says-warrantless-device-searches-border-must-be-limited-to-searches-contraband.shtml [https://perma.cc/P4GN-H997].

¹⁰ *Cano*, 934 F.3d at 1008.

¹¹ *Id.*

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.* The agents claimed that the manual searches were easily conducted because Cano's phone was unlocked. Answering Brief for the United States at 20, *Cano*, 934 F.3d 1002 (9th Cir. 2019) (No. 17-50151).

¹⁵ *Cano*, 934 F.3d at 1008. The Cellebrite download allowed access to "text messages, contacts, call logs, media, and application data." *Id.* at 1008–09. The agents used the results of this search to probe Cano's alleged reason for crossing the border — that he was looking for work at a carpet store — and concluded Cano had not, in fact, placed any calls to San Diego-area carpet stores. *Id.*

¹⁶ *United States v. Cano*, 222 F. Supp. 3d 876, 878 (S.D. Cal. 2016).

¹⁷ *Id.* at 882 (citing *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc)).

¹⁸ *Id.* at 879.

¹⁹ *Id.* at 880.

²⁰ 709 F.3d 952.

²¹ *See id.* at 967–68.

²² *Id.* at 962.

intrusive of the searches — the Cellebrite download search — to be justified under the exception,²³ because even if it were considered a forensic search, the discovery of cocaine provided the reasonable suspicion²⁴ necessary to forgo the warrant.²⁵ Cano was eventually convicted.²⁶

The Ninth Circuit reversed. Writing for a unanimous panel, Judge Bybee²⁷ vacated Cano's conviction after determining that the border officials violated Cano's Fourth Amendment rights and that most of the evidence from their searches should have been suppressed.²⁸ In articulating the appropriate standard for the border search exception, Judge Bybee explicitly extended the *Cotterman* framework to cell phones, holding that manual border searches of cell phones require no suspicion, while forensic searches require reasonable suspicion.²⁹ The court dismissed the notion that the logic of *Riley v. California*,³⁰ which established heightened requirements for cell phone searches incident to arrest,³¹ is equally applicable in the border search context.³² Given the diminished expectation of privacy at the border,³³ Judge Bybee reasoned, *Riley* had not abrogated *Cotterman* and *Cotterman*'s two-tiered suspicion framework properly governed the analysis.³⁴

Turning to the proper scope of the border search exception, Judge Bybee found that because “every border-search case the Supreme Court has decided involved searches to locate *items being smuggled*,’ rather than evidence,”³⁵ only searches directed at “determin[ing] whether the phone contains contraband” were permissible under the exception.³⁶ Searches for evidence of contraband or “border-related crimes” were

²³ *Cano*, 222 F. Supp. 3d at 882.

²⁴ In fact, the court concluded that this discovery not only amounted to reasonable suspicion, but also gave rise to probable cause. *Id.*

²⁵ *Id.* The district court declined to determine whether the third search was “forensic.” *Id.*

²⁶ *Cano*, 934 F.3d at 1010. The first trial resulted in a hung jury and a mistrial; the second trial resulted in a conviction. *Id.*

²⁷ Judge Bybee was joined by Judges Graber and Harpool. Judge Harpool, of the Western District of Missouri, was sitting by designation.

²⁸ *Cano*, 934 F.3d at 1007.

²⁹ *Id.* at 1015–16. *Cotterman* dealt with searches of a laptop. See *United States v. Cotterman*, 709 F.3d 952, 956–57 (9th Cir. 2013) (en banc).

³⁰ 134 S. Ct. 2473 (2014).

³¹ *Riley* required that “officers must generally secure a warrant before conducting such a search.” *Id.* at 2485.

³² See *Cano*, 934 F.3d at 1015.

³³ *Id.* at 1015 (“[T]he Fourth Amendment’s balance of reasonableness is qualitatively different at the international border than in the interior” (quoting *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985))).

³⁴ See *id.* at 1015–16.

³⁵ *Id.* at 1018 (quoting *United States v. Molina-Isidoro*, 884 F.3d 287, 295 (5th Cir. 2018) (Costa, J., specially concurring) (emphasis added)).

³⁶ *Id.* Elsewhere in the opinion, Judge Bybee clarified that “[a]lthough cell phone data cannot hide physical objects, the data can contain *digital contraband*.” *Id.* at 1014 (footnote omitted).

outside the exception's scope.³⁷ Integrating the scope standard and suspicion framework, the court concluded that border officials could conduct warrantless *forensic* searches of cell phones only "when they reasonably suspect that the cell phone contains contraband."³⁸

Under this standard, the court found the first manual search — which verified there were no text messages on the phone — was properly directed at finding contraband, as "[c]hild pornography may be sent via text message."³⁹ The court found the second manual search, however, to be outside the scope because the "recording of the phone numbers and text messages" had "no connection to ensuring that the phone lack[ed] digital contraband."⁴⁰ Nevertheless, the court condoned the perusal of Cano's call log.⁴¹ Noting that "[c]riminals may hide contraband in unexpected places," Judge Bybee found that such a perusal could be necessary to ensure the log did not contain "surreptitious" digital contraband.⁴² Finally, the court held that if the third search — the one conducted with Cellebrite software — was a "forensic search," then it was unreasonable, as the agents could not have reasonably suspected that Cano's phone contained contraband.⁴³

Having found that at least one of the searches violated the Fourth Amendment, the court held the proper remedy was suppression of the evidence, as the "good faith exception" did not apply.⁴⁴ The good faith exception allows for the admission of evidence from an improper search when the search was conducted "in objectively reasonable reliance on binding judicial precedent."⁴⁵ Judge Bybee determined that because *Cotterman* involved a direct search for contraband, it could not have justified the search for *evidence* of future crimes on Cano's phone.⁴⁶

Finally, the court rejected Cano's claim that the government violated his rights under *Brady v. Maryland*⁴⁷ and Rule 16 of the Federal Rules of Criminal Procedure by failing to turn over evidence related to his

³⁷ *Id.* at 1018. The court recognized that this holding created a split with the Fourth Circuit, which had held that the border search exception is "broad enough to accommodate . . . the prevention and disruption of ongoing efforts to export contraband illegally." *Id.* at 1017 (emphasis omitted) (quoting *United States v. Kolsuz*, 890 F.3d 133, 143 (4th Cir. 2018)).

³⁸ *Id.* at 1020.

³⁹ *Id.* at 1019. In a footnote, Judge Bybee explained that he focused his analysis on child pornography because "[m]ost of the cases have involved child pornography" and "the detection-of-contraband justification would rarely seem to apply to an electronic search of a cell phone outside the context of child pornography." *Id.* at 1021 n.13.

⁴⁰ *Id.* at 1019.

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.* at 1021. Like the district court, the court declined to pass on whether the search at issue was in fact a forensic search. *Id.*; *see also* *United States v. Cano*, 222 F. Supp. 3d 876, 882 (S.D. Cal. 2016).

⁴⁴ *Cano*, 934 F.3d at 1022.

⁴⁵ *Id.* at 1021 (quoting *Davis v. United States*, 564 U.S. 229, 239 (2011)).

⁴⁶ *Id.* at 1021–22.

⁴⁷ 373 U.S. 83 (1963).

third-party defense theory.⁴⁸ Because the prosecutors did not have knowledge of, or access to, the documents Cano was requesting, Judge Bybee reasoned, they could not have withheld those documents.⁴⁹

On its face, *Cano*'s narrowing of the border search exception's scope to encompass only cell phone searches directed at finding digital contraband strengthens Fourth Amendment protections.⁵⁰ Yet the court's application of the standard to the two manual searches of Cano's phone reveals that it does little to cabin the practical scope of manual searches, and consequently fails to increase protections for border crossers. Indeed, the interaction of the court's application of the exception with both existing Fourth Amendment doctrine and new technology could allow officers at the border to continue to conduct nearly limitless manual cell phone searches. And the court's analysis of the agents' putatively forensic third search, conducted under the integrated reasonable suspicion of contraband standard, further underscores the lack of protections from manual searches.

The court's analysis of the first manual search demonstrates the extent to which its scope inquiry is susceptible to evasion by pretext. Neither of the border agents' subjective motivations for conducting this search — finding “investigative leads” or searching for “evidence of other things coming across the border”⁵¹ — comported with the court's requirement that cell phone searches be directed at finding contraband itself rather than at finding *evidence* of contraband or other crimes.⁵² But the reasonableness of a government search is determined under an objective standard,⁵³ meaning that a court must uphold objectively reasonable searches even when border agents admit to subjective search motivations outside the permissible scope.⁵⁴ As a result, the court eschewed the agents' subjective motivations and relied instead on its own determination that looking through text messages was objectively within the scope of the exception.⁵⁵ And because such a determination is the end of the inquiry, the manner in which the court conducts its reasonableness analysis becomes all the more important to future courts

⁴⁸ See *Cano*, 934 F.3d at 1022–24. Cano alleged that his cousin, who was a member of a gang involved in drug trafficking, had access to the car where the cocaine was found. *Id.* at 1023–24.

⁴⁹ *Id.* at 1026.

⁵⁰ See sources cited *supra* note 9.

⁵¹ *Cano*, 934 F.3d at 1008 (quoting HSI Agent Petonak).

⁵² The court recognized this in a footnote, but dismissed it as part of its broader determination that “Cano's focus on the officials' subjective motivations is misplaced.” *Id.* at 1016 n.9.

⁵³ *Id.* (citing *Whren v. United States*, 517 U.S. 806, 813 (1996)).

⁵⁴ *Cf. Scott v. United States*, 436 U.S. 128, 138 (1978) (“[T]he fact that the officer does not have the state of mind which is hypothecated by the reasons which provide the legal justification for the officer's action does not invalidate the action taken as long as the circumstances, viewed objectively, justify that action.”).

⁵⁵ See *Cano*, 934 F.3d at 1019.

tasked with implementing this new scope standard.⁵⁶ Yet the *Cano* court provided little explanation for its determination, noting only that text messages are the type of thing that “may” house digital contraband.⁵⁷ In providing guidance only at such a high level of generality, the court did little to deter future pretextual searches.⁵⁸

When the *Cano* court did attempt to draw an administrable line — in its analysis of the second manual search — it did so in a manner that expanded, rather than limited, the universe of rationalizations that could be used to evade the strictures of its scope standard. By finding “record[ing] phone numbers found in the call log” to be outside the scope while allowing officers to “thumb through” the call log,⁵⁹ the court authorized border agents to manually examine the call log of every person passing through the border — without any quantum of individualized suspicion — on the grounds that such an examination objectively constitutes a search for contraband. This exposes a trove of noncontraband digital content, much of it private in nature,⁶⁰ to the gaze of any border agent inclined to look.

And by justifying that line drawing with the generalization that “[c]riminals may hide contraband in unexpected places,” the court potentially extended the permissible range of content that can be “thumb[ed] through” to any app on the phone.⁶¹ Though *Cano* did not cite any authority to support this generalization, there is ample evidence that many smartphone users do, in fact, use apps designed to hide digital contraband.⁶² These “vault apps” can be made to resemble any number

⁵⁶ See Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 526 (2007) (“Fourth Amendment decision making relies heavily on analogies, which means that legal reasoning adopted in one factual setting will tend to be adopted in similar factual settings.”).

⁵⁷ *Cano*, 934 F.3d at 1019 (emphasis added).

⁵⁸ At least one scholar has suggested limiting the scope of underlying government powers as a way of deterring pretextual searches. See James B. Haddad, *Pretextual Fourth Amendment Activity: Another Viewpoint*, 18 U. MICH. J.L. REFORM 639, 651–53 (1985) (“A narrowing of police power would restrict opportunity and incentive for abuse.” *Id.* at 652.). This analysis overlooks a case where — as here — the standard through which the scope is narrowed is itself susceptible to pretext.

⁵⁹ *Cano*, 934 F.3d at 1019.

⁶⁰ See Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant-Appellant at 4–10, *Cano*, 934 F.3d 1002 (9th Cir. 2019) (No. 17-50151).

⁶¹ *Cano*, 934 F.3d at 1019.

⁶² See, e.g., Katie Rogers, *The Vault Apps that Keep Sexes a Secret*, N.Y. TIMES (Nov. 6, 2015), <https://nyti.ms/1kztYJw> [<https://perma.cc/QT8S-D322>] (reporting such apps have been used by teenagers to store nude images and noting one such app had “more than 1,500 individual reviews” and was “the 28th most downloaded photo and video app on the App Store”); Shereen Siewert, *Marshfield Man Sentenced to Prison in 2 Separate Child Sex Cases*, WAUSAU PILOT & REV. (June 12, 2019), <https://wausaupilotandreview.com/2019/06/12/marshfield-man-sentenced-to-prison-in-2-separate-child-sex-cases> [<https://perma.cc/4NTW-MVVL>] (noting conviction of man who used a vault app to store child pornography).

of commonplace apps — from calendars to calculators⁶³ — that would never be thought to house contraband.⁶⁴ Operating under *Cano*, government officials familiar with vault apps could credibly claim that manually examining the contents of *every application* on a cell phone was part of a dutiful search for “surreptitious images or videos.”⁶⁵ Such an outcome, which creates a universal post hoc rationalization for cell phone searches, implicitly authorizes near-boundless searches.

Furthermore, application of the *Cano* standard could bring the contents of a phone’s call log or other apps into the plain view of a border official, thus paradoxically triggering *seizure* of noncontraband that, in theory, could not be *searched for* under *Cano*’s scope conception.⁶⁶ Under the plain view doctrine, law enforcement officials may seize plainly viewable evidence to which they have a “lawful right of access,”⁶⁷ so long as its incriminating nature is “immediately apparent.”⁶⁸ In *United States v. Seljan*,⁶⁹ the Ninth Circuit relied on the plain view doctrine to uphold the seizure of a letter containing “evidence of possible pedophilia” by customs agents searching for undeclared currency.⁷⁰ Though such a letter — if stored digitally — would be outside the scope of the border search exception under *Cano*, as it would be merely evidence of contraband,⁷¹ the officers would be justified in “thumb[ing] through” it — just as they were in perusing *Cano*’s call log — and its seizure could still be permitted under the plain view doctrine, just as in *Seljan*.⁷²

⁶³ Molly McLaughlin, *The 9 Best Vault Apps of 2020*, LIFEWIRE (Mar. 25, 2020), <https://www.lifewire.com/best-vault-apps-4172048> [<https://perma.cc/36ZD-WKM7>].

⁶⁴ See Rogers, *supra* note 62.

⁶⁵ *Cano*, 934 F.3d at 1019.

⁶⁶ The plain view doctrine was not a factor in *Cano* itself. Though the *Cano* court speculated that the plain view doctrine might have justified the agents’ recording of the phone numbers in *Cano*’s call log — something the court deemed impermissible under the scope analysis — it declined to pass on this issue, as the government did not raise the argument in its briefs. See *id.* at 1020 n.11.

⁶⁷ *Horton v. California*, 496 U.S. 128, 137 (1990). Here, the border search exception would provide the right of access. See *United States v. Bulacan*, 156 F.3d 963, 968 (9th Cir. 1998) (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 465 (1971) (plurality opinion)) (“The initial intrusion can be justified . . . by one of the recognized exceptions of the warrant requirement.”).

⁶⁸ *Horton*, 496 U.S. at 136 (quoting *Coolidge*, 403 U.S. at 466 (plurality opinion)).

⁶⁹ 547 F.3d 993 (9th Cir. 2008) (en banc).

⁷⁰ *Id.* at 1005.

⁷¹ See *Cano*, 934 F.3d at 1017.

⁷² See *Seljan*, 547 F.3d at 1005–06 (upholding seizure on the basis of “precedents involving the plain view doctrine,” *id.* at 1005, given that the officer had a “lawful right of access” to the letter, *id.* at 1006 (quoting *Horton*, 496 U.S. at 137), and that its incriminating nature was “immediately apparent,” *id.* (quoting *Bulacan*, 156 F.3d at 968)). *But cf.* *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1179–80 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring) (offering nonbinding guidance that magistrate judges reviewing warrant applications “should insist that the government waive reliance upon the plain view doctrine in digital evidence cases,” *id.* at 1180); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 576–84 (2005) (arguing the plain view doctrine should be narrowed for digital searches).

The court's analysis of the third search, however, shows there is a way to implement a scope standard that is resilient to these doctrinal challenges and that more effectively limits warrantless border searches to those within the exception's scope. Evaluating the putatively forensic search, the court determined that the agents did not have the reasonable suspicion of contraband necessary to conduct a warrantless search.⁷³ This determination ended the inquiry.⁷⁴ Tethering the scope standard to the suspicion standard in this way moves the focus of the analysis earlier — to before the initiation of the search. This approach prevents agents not searching for contraband from ever obtaining a “lawful right of access” to the phone's content, minimizing the chances of an outside-the-scope seizure under the plain view doctrine. And where this tethered analysis ends the inquiry altogether — as it did here — it obviates the need for the pretext-facilitating “objective” analysis of specific search techniques. This approach puts the lack of protection offered by the standard for manual searches — which have no suspicion requirement to which their scope analysis could be tethered⁷⁵ — into sharp relief.⁷⁶

The *Cano* court's analysis of the first two searches thus demonstrates that its newly announced scope standard provides minimal protection from manual cell phone searches at the border. Without the requirement of reasonable suspicion of contraband, the manual search scope standard is enforced only through the easily circumvented objective purpose analysis. Though the *Cano* court sought to ensure that “border officials [were] limited to searching for contraband only,”⁷⁷ *Cano*'s attempt to implement that command came closer to perpetuating a paradigm where “at the border, anything goes.”⁷⁸

⁷³ See *Cano*, 934 F.3d at 1021 (finding that although the agents “had reason to suspect that *Cano*'s phone would contain evidence leading to additional drugs, the record does not give rise to any objectively reasonable suspicion that the digital data in the phone contained contraband”).

⁷⁴ *Id.*

⁷⁵ *Id.* at 1016.

⁷⁶ Though beyond the scope of this comment, the extent of this disparity lends support for extending the reasonable suspicion of contraband standard to all border searches of cell phones. No circuit has adopted this approach, see *United States v. Molina-Isidoro*, 884 F.3d 287, 293 (5th Cir. 2018), but the District Court for the District of Massachusetts has embraced a similar standard, see *Alasaad v. Nielsen*, No. 17-cv-11730, 2019 WL 5899371, at *15 (D. Mass. Nov. 12, 2019) (citing *Cano* for the proposition that the reasonable suspicion standard must be tethered to the scope of the exception). Given the existing circuit splits over border search doctrine, see Note, *supra* note 6, and the delicate balancing of privacy and public safety required in this area, it may be that Congress is best suited to the task of sustainably bolstering *Cano*'s scope limitation. Cf. *United States v. Jones*, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring in the judgment) (“A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.”). In 2018, a bipartisan Senate bill proposed a reasonable suspicion standard for manual searches of electronic devices at the border. S. 2462, 115th Cong. § 2(b) (2018). A revised version, requiring reasonable suspicion of contraband, could be the ideal vehicle to give teeth to the exception's scope.

⁷⁷ *Cano*, 934 F.3d at 1019.

⁷⁸ *United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008) (en banc) (declining to hold that “at the border, anything goes”).