CONSTITUTIONAL LAW — FOURTH AMENDMENT — NINTH CIRCUIT HOLDS FORENSIC SEARCH OF LAPTOP SEIZED AT BORDER REQUIRES SHOWING OF REASONABLE SUSPICION. — *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc).

Technological innovation has outpaced the evolution of Fourth Amendment jurisprudence, creating new conflicts between the opposing interests of the government in security and the individual in privacy.[1] Among the questions that have emerged is whether the rise of digital media devices as international travel companions[2] requires recasting the long-recognized border search exception to the Fourth Amendment's prohibition on unreasonable searches.[3] Recently, in *United States v. Cotterman*,[4] the Ninth Circuit answered in the affirmative, holding that border agents need reasonable suspicion of criminal activity to justify a forensic search of a laptop seized at the border.[5] While the sovereign's interest in security is "at its zenith at the international border,"[6] the court concluded that, because a laptop's contents are so personal and forensic searches so "painstaking,"[7] an exception to the border search doctrine was warranted.[8] In reaching this conclusion, the court correctly recognized that forensic searches pose a threat of a fundamentally different order to personal privacy, but it could have strengthened its innovative holding by focusing on the idea that such searches are conducted in a "particularly offensive manner."

In April 2007, Howard Cotterman and his wife attempted to reenter the United States at an Arizona port of entry following a vacation in Mexico.[9] During primary inspection, the Treasury Enforcement Communication System (TECS)[10] returned a hit on Cotterman's pass-

---

[1] *See* Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1, 5, 40–41 (2011); *cf.* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 838 (2004) ("Most existing Fourth Amendment rules . . . offer only relatively modest privacy protection in new technologies.").

[2] Christine A. Coletta, Note, *Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment*, 48 B.C. L. REV. 971, 973 (2007).

[3] U.S. CONST. amend. IV. Searches at the border are regarded as per se reasonable by virtue of where they occur, *see* United States v. Ramsey, 431 U.S. 606, 616 (1977), unless they are (1) conducted in a "particularly offensive manner," *id.* at 618 n.13; *see also* United States v. Flores-Montano, 541 U.S. 149, 154 n.2 (2004); (2) "highly intrusive searches of the person," *Flores-Montano*, 541 U.S. at 152; or (3) destructive of property, *see id.* at 156.

[4] 709 F.3d 952 (9th Cir. 2013) (en banc).

[5] *Id.* at 968.

[6] *Id.* at 960 (quoting *Flores-Montano*, 541 U.S. at 152) (internal quotation mark omitted).

[7] *Id.* at 962.

[8] *Id.* at 962–63, 967–68.

[9] *Id.* at 957.

[10] TECS provides border officials with access to travel histories and law enforcement records in order to assist them in screening individuals for admission into the country. *See id.* at 957 n.3.

port, notifying officers that he might be involved in child sex tourism.[11] After the TECS alert, agents conducted a secondary search of Cotterman's car, finding two laptops and three digital cameras.[12] An agent manually inspected the devices and found password-protected files but no readily accessible child pornography.[13] Though the Cottermans were permitted to leave the border crossing, agents retained both laptops and one camera and drove the devices 170 miles to an Immigration and Customs Enforcement (ICE) office in Tucson for further inspection.[14] While ICE released the camera the next day, it retained the laptops so that forensic software could examine copies of their hard drives overnight.[15] The next evening, an ICE forensic examiner found seventy-five images of child pornography in the "unallocated space" of Cotterman's laptop.[16] Three days later, the agent bypassed the laptop's security and opened twenty-three password-protected files, finding 378 more such images.[17]

After a federal grand jury indicted him on various child pornography charges,[18] Cotterman moved to suppress the results of ICE's search on the ground that it was a "non-routine border search requiring reasonable suspicion."[19] Magistrate Judge Pyle recommended the motion be granted,[20] but did so on the ground that the forensic review, occurring two days and 170 miles from the crossing, was an "extended border search" for which reasonable suspicion was needed.[21] Agreeing that this burden had not been met, District Judge Collins granted the motion.[22] The United States appealed, arguing that it need not show reasonable suspicion because the border search doctrine justified both

---

[11] *Id.* at 957. Cotterman was flagged because he had a 1992 conviction for sexual conduct with a minor, he was a registered sex offender, and he frequently traveled abroad. *Id.* at 957–58.

[12] *Id.* at 957.

[13] *Id.* at 957–58.

[14] *Id.* at 958.

[15] *Id.*

[16] *Id.* "Unallocated space" is "where the computer stores files that the user ostensibly deleted and maintains other 'deleted' files retrieved from web sites the user has visited." *Id.* at 965.

[17] *Id.* at 959. ICE discovered hundreds more images and videos in the ensuing months. *Id.*

[18] *Id.*

[19] United States v. Cotterman, No. CR 07-1207-TUC-RCC, 2009 WL 465028, at *3 (D. Ariz. Feb. 24, 2009).

[20] *Id.* at *10.

[21] *Id.* at *9. An extended border search is "any 'search away from the border where entry is not apparent,' but where the dual requirements of reasonable certainty of a recent border crossing and reasonable suspicion of criminal activity are satisfied." United States v. Guzman-Padilla, 573 F.3d 865, 878–79 (9th Cir. 2009) (citation omitted) (quoting United States v. Corral-Villavicencio, 753 F.2d 785, 788 (9th Cir. 1985)). Since a person regains an expectation of privacy upon clearing the border, an extended border search involves a greater intrusion "on legitimate expectations of privacy than an ordinary border search" and must be justified with reasonable suspicion. United States v. Abbouchi, 502 F.3d 850, 855 (9th Cir. 2007).

[22] *Cotterman*, 2009 WL 465028, at *1.

the initial review *and* the decision to transfer the laptop to complete the search.[23]

A divided Ninth Circuit panel reversed and remanded.[24] Writing for the panel, Judge Tallman[25] deemed the extended border search doctrine inapposite.[26] Because his laptop was seized at the border and held thereafter, Cotterman did not have — and the act of moving the laptop elsewhere did not create — the type of reasonable expectation of privacy in its contents that would require particularized suspicion.[27] Judge Tallman also concluded that the manner of the search was not sufficiently offensive to overcome the presumption against requiring reasonable suspicion for border searches.[28] The Ninth Circuit subsequently ordered rehearing en banc.[29]

Sitting en banc, the Ninth Circuit once again reversed the district court's ruling.[30] Writing for the court, Judge McKeown[31] also vacated the suppression order, but only after taking the opposite position with regard to the pertinent suspicion standard.[32] Specifically, Judge McKeown held that ICE needed reasonable suspicion to "strip search"[33] Cotterman's laptop.[34] The court explained that data stored on digital media, often "reflect[ing] our most private thoughts and activities," constitute personal "papers," the security of which is protected by the Fourth Amendment.[35] The amount of data carried on digital media, and the fact that such devices often retain confidential data "beyond the perceived point of erasure,"[36] means that most travelers have no choice but to expose "the most intimate details of [their] lives" to border authorities.[37] Given its unique capacity to "mine every last

---

[23] United States v. Cotterman, 637 F.3d 1068, 1074 (9th Cir. 2011). The appeal did not attack the district court's finding that the evidence did not establish "reasonable particularized suspicion." *Id.*

[24] *Id.* at 1070.

[25] Judge Tallman was joined by Judge Rawlinson.

[26] *Cotterman*, 637 F.3d at 1076 (noting that the border search doctrine has often been applied to searches that are temporally and spatially removed from the actual physical border).

[27] *Id.* at 1077. Writing in dissent, Judge Fletcher argued that "authorizing a generalized computer forensic search (untethered to any particularized suspicion) permits . . . the type of generalized fishing expeditions" prohibited by the Fourth Amendment. *Id.* at 1084 (Fletcher, J., dissenting).

[28] *Id.* at 1079–83 (majority opinion). Judge Tallman also held the other two exceptions to the border search doctrine to be inapplicable since the search of Cotterman's laptop was neither destructive nor a "highly intrusive search[] of the person." *Id.* at 1080.

[29] United States v. Cotterman, 673 F.3d 1206, 1207 (9th Cir. 2012).

[30] *Cotterman*, 709 F.3d at 957.

[31] Judge McKeown was joined by Chief Judge Kozinski and Judges Thomas, Wardlaw, Fisher, Gould, Murguia, and Christen.

[32] *See Cotterman*, 709 F.3d at 957. Judge McKeown agreed with the prior panel, however, that ICE's forensic examination of Cotterman's laptop was not an extended border search. *Id.* at 962.

[33] *Id.* at 966.

[34] *Id.* at 968.

[35] *Id.* at 957.

[36] *Id.* at 965.

[37] *Id.* at 964.

piece of data on [such] devices,"[38] a forensic search "intru[des] upon personal privacy and dignity" to a degree "requir[ing] a showing of reasonable suspicion."[39] Nevertheless, the court found the requisite suspicion in the "totality of the circumstances."[40]

Judge Callahan concurred in part, dissented in part, and concurred in the judgment.[41] Rejecting the court's new categorical rule,[42] Judge Callahan admonished the majority for relying on a fallacious view that "electronic devices deserve special consideration because they are ubiquitous and can store vast quantities of personal information."[43] In her view, the Supreme Court has distinguished only between border searches of persons and property, not between types of property, resisting the idea that "the reasonableness of a search turn[s] on the nature of the property being searched"[44] and "refus[ing] to adopt a sliding 'intrusiveness' scale for border searches of property."[45] Border searches of digital media, like those of any container, are presumed to be reasonable, and nothing warranted a departure from that doctrine.[46] In holding otherwise, the majority forces border agents to choose between protecting the country from crime or themselves from *Bivens* actions.[47]

Judge M. Smith dissented,[48] echoing many of Judge Callahan's concerns while criticizing the majority for creating a circuit split and making "a legal bouillabaisse out of the previously unambiguous bor-

---

[38] *Id.* at 967.

[39] *Id.* at 968.

[40] *Id.* at 970. Despite the government's initial failure to raise the issue, Judge McKeown addressed whether reasonable suspicion existed here because (1) Cotterman would not be prejudiced since both parties had been asked for and had submitted supplemental briefs; and (2) determining the applicable standard — "no suspicion, reasonable suspicion or probable cause," *id.* at 960 — was necessary for de novo review of "whether a warrantless search was reasonable under the Fourth Amendment," *id.* at 959–60. Judge McKeown found reasonable suspicion in the agents' awareness of the TECS alert, Mexico's reputation for sex tourism, Cotterman's prior sex offense and frequent travels abroad, and the presence of password-protected files. *Id.* at 968–70.

[41] Judge Callahan was joined in full by Judge Clifton. Judge M. Smith joined in all but Part II.A.

[42] *See Cotterman*, 709 F.3d at 978 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment) ("[N]o court has ever erected so categorical a rule . . . .").

[43] *Id.* at 975.

[44] *Id.* at 980.

[45] *Id.* at 975–76.

[46] *See id.* at 974–76. Judge Callahan nevertheless concurred that reasonable suspicion existed here. *See id.* at 971. Only Judge Smith dissented on this point. *Id.* at 994 (Smith, J., dissenting).

[47] *See id.* at 979 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment). *See generally* Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971) (holding that victim of warrantless search has a federal cause of action for damages against offending agents under Fourth Amendment).

[48] Judges Clifton and Callahan joined in Part I, agreeing that reasonable suspicion was not needed for forensic searches of laptops at the border. *Cotterman*, 709 F.3d at 981–88 (Smith, J., dissenting).

der search doctrine."[49] Judge Smith departed from his colleagues, however, by endorsing the district court's conclusion that ICE had carried out an extended border search.[50] In his view, most of the factors cited by the majority were "far too generalized to provide even an indicia of suspicion."[51] After initial searches and interviews corroborated the Cottermans' vacation story, the mere presence of a password-protected file did not establish reasonable suspicion.[52]

*Cotterman* spins a familiar tale: one of courts struggling to adapt Fourth Amendment principles born of an analog world to a digital age.[53] For years, a judicial aversion to adopting different Fourth Amendment rules for emerging technologies[54] has manifested itself in opinions — ignoring the calls of many scholars[55] — refusing to recognize an electronic-media exception to the border search doctrine,[56] even in cases of forensic searches.[57] *Cotterman* was the first case in which a circuit court asked whether forensic border searches of digital media are searches of a different order. Unfortunately, while it finally asked the right question, the majority undercut its own analysis by being needlessly vague about the doctrinal basis for its effort to meet technological change with jurisprudential innovation.

Individual privacy rights are not extinguished at the border; rather, the Fourth Amendment balance simply has been "struck much more favorably to the Government" in that context.[58] In cases involving manual searches of laptops at the border, courts have held, given precedent that the *nature of the property* being searched is not independently relevant to the inquiry, that the vast storage capacity of laptops is insufficient to tip the balance back in favor of a suspicion

---

[49] *Id.* at 981. Similarly to Judge Callahan, Judge Smith rejected as "artificial and arbitrary" the idea that "the mere process of digitalizing our diaries and work documents somehow increases the 'sensitive nature' of the data therein." *Id.* at 987 (emphasis omitted).

[50] *See id.* at 990.

[51] *Id.* at 992.

[52] *Id.* at 994.

[53] *See* Benjamin J. Rankin, Note, *Restoring Privacy at the Border: Extending the Reasonable Suspicion Standard for Laptop Border Searches*, 43 COLUM. HUM. RTS. L. REV. 301, 347–48 (2011).

[54] *See, e.g.*, United States v. Giberson, 527 F.3d 882, 887–89 (9th Cir. 2008) (rejecting the idea that computers warrant special Fourth Amendment protections); United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007) (holding a warrant unnecessary to search a cell phone pursuant to arrest); *cf.* Kyllo v. United States, 533 U.S. 27, 41 (2001) (Stevens, J., dissenting) (calling a bright-line rule based on technology type "unnecessary, unwise, and inconsistent with the Fourth Amendment").

[55] *See* Nicole Kolinski, United States v. Arnold*: Legally Correct but Logistically Impractical*, 6 J.L. ECON. & POL'Y 31, 32 (2009) (noting that most scholars would require reasonable suspicion). *But see* Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1110–17 (2009) (arguing against special search rules for laptops).

[56] *E.g.*, United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007).

[57] *See* United States v. Ickes, 393 F.3d 501, 505–07 (4th Cir. 2005).

[58] *Cotterman*, 709 F.3d at 960 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 540 (1985)) (internal quotation marks omitted).

requirement.[59] Like Judge Callahan's opinion,[60] the only cases from other circuits to address whether border searches of electronic media require suspicion, *United States v. Linarez-Delgado*[61] and *United States v. Ickes*,[62] grounded themselves in the reasoning of these manual-search cases, asking only whether the media themselves are special for border search purposes irrespective of the search mechanism.[63] As these courts concluded and Judge McKeown accepted, the answer *to that question* is "no."[64] What Judge McKeown adeptly recognized, though, is that *Cotterman* raised a different, as yet unresolved question: is there anything unique about the *type of search* at issue that alters the Fourth Amendment balance at the border?[65]

The majority rightly answered in the affirmative. The type of manual review at issue in cases like *United States v. Arnold*[66] — which involved turning the device on and perusing visible files[67] — is analogous to searches of other containers insofar as a traveler, when packing, can choose what material to subject to scrutiny.[68] But a forensic search is more akin to "reading a diary line by line looking for mention of criminal activity — plus looking at everything the writer may have erased."[69] Analysts can comb through the laptop's entire digital profile, exposing not just files one consciously chose to carry, but also deleted files and troves of data that the user did not know existed and over which she had no control.[70] As the majority noted, what makes the search in *Cotterman* particularly invasive is not just that laptops are "warehouses full of . . . the most intimate details of our

---

[59] *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1008–10 (9th Cir. 2008); *see also Cotterman*, 709 F.3d at 976–77 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment) (reviewing the relevant case law).

[60] *See Cotterman*, 709 F.3d at 976 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment) ("The two courts of appeals" that have "address[ed] whether electronic devices deserve special consideration have correctly concluded that they do not.").

[61] 259 F. App'x 506.

[62] 393 F.3d 501.

[63] *See Linarez-Delgado*, 259 F. App'x at 507–08; *Ickes*, 393 F.3d at 505–08.

[64] *But see* Rasha Alzahabi, Note, *Should You Leave Your Laptop at Home When Traveling Abroad? The Fourth Amendment and Border Searches of Laptop Computers*, 41 IND. L. REV. 161, 178–86 (2008) (arguing that unique qualities of laptops justify a reasonable suspicion requirement).

[65] *Cotterman*, 709 F.3d at 961 ("The . . . question we confront is the reasonableness [of a warrantless] forensic examination that comprehensively analyzed the hard drive of the computer.").

[66] 533 F.3d 1003 (9th Cir. 2008).

[67] *Id.* at 1005, 1007–08.

[68] *See Cotterman*, 709 F.3d at 965 ("When packing traditional luggage, one is accustomed to deciding what papers to take and what to leave behind.").

[69] *Id.* at 962–63.

[70] For a discussion of the technical process of forensically examining a computer, see Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 540–43 (2005). Software is used to create a "read only" copy of the entire drive so that it may be searched without altering the original data. *Id.* Deleted files can often be recovered because "deleting" a file does not scrub it from the drive, but merely marks its memory "clusters" as available for future use. *Id.* at 542.

lives,"[71] but that the search is akin to one "reveal[ing] not only what [a] bag contained on [a specific trip], but everything it had ever carried."[72]

Unfortunately, while the court reached the right answer, it was vague as to how it got there. At heart, the border search doctrine simply reflects a presumption that the Fourth Amendment balance tilts in the sovereign's favor at the border, a fact made clear by the Supreme Court's announcement of three exceptions to the doctrine: reasonable suspicion may be required for border searches that are (1) highly intrusive searches of the person, (2) destructive of property, or (3) conducted in a particularly offensive manner.[73] In *Cotterman*, the majority vacillated between the first and third exceptions, seemingly merging them.[74] In the majority's hands, "intrusiveness" and "offensiveness" became abstract, interchangeable terms that characterized the degree to which a search impedes "dignity and privacy interests."[75]

The court's ambivalence undermines its analysis and betrays a failure to explicitly choose the one doctrinal door that the Supreme Court had left open to it. In merging the exceptions, the majority expanded the "highly intrusive" exception far beyond its origin: the exception distinguishes between "persons" and "effects," addressing only "highly intrusive searches *of the person*."[76] Try as the majority might, laptop searches — like searches of trucks — cannot be considered searches *of the person* except in a metaphysical sense.[77] Given the Supreme Court's suggestion that these exceptions are narrow — it has required reasonable suspicion for a border search only once[78] — the "highly intrusive" exception is a shaky foundation for the majority's holding. The court should have focused solely on the third exception because, while the Supreme Court has yet to fit a case within this exception, it has deliberately "le[ft] open the question 'whether, and under what circumstances, a border search might be deemed "unreasonable" because of the particularly offensive *manner* in which it is carried out.'"[79]

---

[71] *Cotterman*, 709 F.3d at 964.

[72] *Id.* at 965.

[73] United States v. Flores-Montano, 541 U.S. 149, 152–56 & n.2 (2004).

[74] *See Cotterman*, 709 F.3d at 973 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment). *Compare id.* at 963 (majority opinion) (framing analysis in terms of offensiveness), *with id.* at 966 ("An exhaustive forensic search of a copied laptop hard drive intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border.").

[75] *Id.* at 966; *see also id.* at 962–68.

[76] *Flores-Montano*, 541 U.S. at 152 (emphasis added) ("But the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person — dignity and privacy interests of the person being searched — simply do not carry over to vehicles.").

[77] *See id.*

[78] United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985) (holding reasonable suspicion was required for twenty-four-hour detention of suspected alimentary canal smuggler).

[79] *Flores-Montano*, 541 U.S. at 154 n.2 (emphasis added) (quoting United States v. Ramsey, 431 U.S. 606, 618 n.13 (1977)).

By focusing on the "offensive manner" exception and building an analytical framework around the "exhaustive" and "exploratory" nature of forensic searches, the majority could have strengthened its holding. Courts have evaluated the offensiveness of a search in terms of the time of day it was conducted and the regularity with which people are singled out for inspection.[80] But the inquiry need not be restricted to such factors. While the mere fact that the searched property holds much data does not make the manner of its search offensive,[81] courts could consider the exhaustive and exploratory nature of a search as part of the "manner" inquiry.[82] In fact, the Supreme Court seemingly endorsed consideration of these factors by citing two cases when it announced this exception[83]: *Kremen v. United States*[84] and *Go-Bart Importing Co. v. United States*.[85] In *Kremen*, the Court held that an *exhaustive* warrantless search of a cabin, whose entire contents were transported 200 miles for review, violated the Fourth Amendment.[86] In *Go-Bart*, the Court struck down a warrantless office search as "a lawless invasion . . . and a general *exploratory* search in the hope that evidence of crime might be found."[87] The search in *Cotterman* is analogous: it was not a narrowly tailored search for specific files, but rather an exhaustive review of the entire digital profile, poised to explore every byte.[88] Given that forensic software is uniquely capable of exposing sensitive personal data, this type of unfocused, exploratory forensic search should require particularized suspicion. Such a ruling, though, likely must be based on the "offensive manner" exception.

When it comes to forensic border searches of laptops, a circuit has now asked and answered the right question. In adjusting the border's Fourth Amendment balance, though, the Ninth Circuit tried to walk through two doors at once where only one was open. Whether or not *Cotterman* survives the Supreme Court's distaste for categorical rules at the border,[89] for now it remains a tribute to the idea that it is "foolish to contend that the degree of privacy secured . . . by the Fourth Amendment has been entirely unaffected by the advance of technology."[90]

---

[80] *See, e.g.*, United States v. Ortiz, 422 U.S. 891, 894–95 (1975).

[81] *See* United States v. Arnold, 533 F.3d 1003, 1010 (9th Cir. 2008).

[82] *See* Aaron McKnight, Note, *Privacy Rights Left Behind at the Border: The Exhaustive, Exploratory Searches Effectuated in* United States v. Cotterman, 2012 B.Y.U. L. REV. 591, 600–01.

[83] *See Ramsey*, 431 U.S. at 618 n.13. Judge McKeown also cited both cases when introducing the "particularly offensive" manner exception in her analysis. *See Cotterman*, 709 F.3d at 963.

[84] 353 U.S. 346 (1957).

[85] 282 U.S. 344 (1931).

[86] *Kremen*, 353 U.S. at 347.

[87] *Go-Bart*, 282 U.S. at 358 (emphasis added).

[88] *See* McKnight, *supra* note 82, at 604–05.

[89] *See Cotterman*, 709 F.3d at 978 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment).

[90] Kyllo v. United States, 533 U.S. 27, 33–34 (2001).