

FOR PUBLICATION**UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

UNITED STATES OF AMERICA,
Plaintiff-Appellant,

v.

HOWARD WESLEY COTTERMAN,
Defendant-Appellee.

No. 09-10139

D.C. No.
4:07-cr-01207-
RCC-CRP-1

OPINION

Appeal from the United States District Court
for the District of Arizona
Raner C. Collins, District Judge, Presiding

Argued and Submitted En Banc
June 19, 2012—Pasadena, California

Filed March 8, 2013

Before: Alex Kozinski, Chief Judge, Sidney R. Thomas, M.
Margaret McKeown, Kim McLane Wardlaw, Raymond C.
Fisher, Ronald M. Gould, Richard R. Clifton, Consuelo M.
Callahan, Milan D. Smith, Jr., Mary H. Murguia, and
Morgan Christen, Circuit Judges.¹

Opinion by Judge McKeown;
Partial Concurrence and Partial Dissent by Judge Callahan;
Dissent by Judge Milan D. Smith, Jr.

¹ Judge Betty B. Fletcher was a member of the en banc panel but passed away after argument of the case. Judge Wardlaw was drawn as her replacement.

SUMMARY*

Criminal Law

The en banc court reversed the district court's order suppressing evidence of child pornography obtained from a forensic examination of the defendant's laptop, which was seized by agents at the U.S.-Mexico border in response to an alert based in part on a prior conviction for child molestation.

The en banc court explained that a border search of a computer is not transformed into an "extended border search" requiring particularized suspicion simply because the device is transported and examined beyond the border. The en banc court wrote that the fact that the forensic examination occurred 170 miles away from the border did not heighten the interference with the defendant's privacy, and the extended border search doctrine does not apply, in this case in which the defendant's computer never cleared customs and the defendant never regained possession.

The en banc court held that the forensic examination of the defendant's computer required a showing of reasonable suspicion, a modest requirement in light of the Fourth Amendment. The en banc court wrote that it is the comprehensive and intrusive nature of forensic examination – not the location of the examination – that is the key factor triggering the requirement of reasonable suspicion here. The en banc court wrote that the uniquely sensitive nature of data on electronic devices, which often retain information far

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

beyond the perceived point of erasure, carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property.

The en banc court held that the border agents had reasonable suspicion to conduct an initial search at the border (which turned up no incriminating material) and the forensic examination. The en banc court wrote that the defendant's Treasury Enforcement Communication System alert, prior child-related conviction, frequent travels, crossing from a country known for sex tourism, and collection of electronic equipment, plus the parameters of the Operation Angel Watch program aimed at combating child sex tourism, taken collectively, gave rise to reasonable suspicion of criminal activity.

The en banc court wrote that password protection of files, which is ubiquitous among many law-abiding citizens, will not in isolation give rise to reasonable suspicion, but that password protection may be considered in the totality of the circumstances where, as here, there are other indicia of criminal activity. The en banc court wrote that the existence of password-protected files is also relevant to assessing the reasonableness of the scope and duration of the search of the defendant's computer.

The en banc court concluded that the examination of the defendant's electronic devices was supported by reasonable suspicion and that the scope and manner of the search were reasonable under the Fourth Amendment.

Concurring in part, dissenting in part, and concurring in the judgment, Judge Callahan (with whom Judge Clifton

joined and with whom Judge M. Smith joined as to all but Part II.A) wrote that the majority's new rule requiring reasonable suspicion for any thorough search of electronic devices entering the United States flouts more than a century of Supreme Court precedent, is unworkable and unnecessary, and will severely hamstring the government's ability to protect our borders.

Judge M. Smith (with whom Judges Clifton and Callahan joined with respect to Part I) dissented. Judge Smith wrote that the majority's decision to create a reasonable suspicion requirement for some property searches at the border so muddies current border search doctrine that border agents will be left to divine on an ad hoc basis whether a property search is sufficiently "comprehensive and intrusive" to require suspicion, or sufficiently "unintrusive" to come within the traditional border search exception. Judge Smith also wrote that the majority's determination that reasonable suspicion exists under the exceedingly weak facts of this case undermines the liberties of U.S. citizens generally – not just at the border, and not just with regard to our digital data – but on every street corner, in every vehicle, and wherever else we rely on the doctrine of reasonable suspicion to safeguard our legitimate privacy interests.

COUNSEL

Dennis K. Burke, Christina M. Cabanillas, Carmen F. Corbin, John S. Leonardo, John J. Tuchi, United States Attorney's Office for the District of Arizona, Tucson, Arizona, for Appellant.

William J. Kirchner, Law Office of Nash & Kirchner, P.C., Tucson, Arizona, for Appellee.

David M. Porter, Malia N. Brink, National Association of Criminal Defense Lawyers, Washington, D.C.; Michael Price, Brennan Center for Justice, New York, New York; Hanni M. Fakhoury, Electronic Frontier Foundation, San Francisco, California, for Amicus Curiae National Association of Criminal Defense Lawyers and Electronic Frontier Foundation.

Christopher T. Handman, Mary Helen Wimberly, Hogan Lovells US LLP, Washington, D.C.; Sharon Bradford Franklin, The Constitution Project, Washington, D.C., for Amicus Curiae The Constitution Project.

OPINION

McKEOWN, Circuit Judge:

Every day more than a million people cross American borders, from the physical borders with Mexico and Canada to functional borders at airports such as Los Angeles (LAX), Honolulu (HNL), New York (JFK, LGA), and Chicago (ORD, MDW). As denizens of a digital world, they carry with them laptop computers, iPhones, iPads, iPods, Kindles,

Nooks, Surfaces, tablets, Blackberries, cell phones, digital cameras, and more. These devices often contain private and sensitive information ranging from personal, financial, and medical data to corporate trade secrets. And, in the case of Howard Cotterman, child pornography.

Agents seized Cotterman's laptop at the U.S.-Mexico border in response to an alert based in part on a fifteen-year-old conviction for child molestation. The initial search at the border turned up no incriminating material. Only after Cotterman's laptop was shipped almost 170 miles away and subjected to a comprehensive forensic examination were images of child pornography discovered.

This watershed case implicates both the scope of the narrow border search exception to the Fourth Amendment's warrant requirement and privacy rights in commonly used electronic devices. The question we confront "is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). More specifically, we consider the reasonableness of a computer search that began as a cursory review at the border but transformed into a forensic examination of Cotterman's hard drive.

Computer forensic examination is a powerful tool capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on web sites. But while technology may have changed the expectation of privacy to some degree, it has not eviscerated it, and certainly not with respect to the gigabytes of data regularly maintained as private and confidential on digital devices. Our Founders were indeed prescient in specifically incorporating "papers" within the Fourth Amendment's guarantee of "[t]he right of

the people to be secure in their persons, houses, papers, and effects.” U.S. Const. amend. IV. The papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities.

Although courts have long recognized that border searches constitute a “historically recognized exception to the Fourth Amendment’s general principle that a warrant be obtained,” *United States v. Ramsey*, 431 U.S. 606, 621 (1977), reasonableness remains the touchstone for a warrantless search. Even at the border, we have rejected an “anything goes” approach. *See United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008) (en banc).

Mindful of the heavy burden on law enforcement to protect our borders juxtaposed with individual privacy interests in data on portable digital devices, we conclude that, under the circumstances here, reasonable suspicion was required for the forensic examination of Cotterman’s laptop. Because border agents had such a reasonable suspicion, we reverse the district court’s order granting Cotterman’s motion to suppress the evidence of child pornography obtained from his laptop.

I. FACTUAL BACKGROUND AND PROCEDURAL HISTORY²

Howard Cotterman and his wife were driving home to the United States from a vacation in Mexico on Friday morning, April 6, 2007, when they reached the Lukeville, Arizona, Port of Entry. During primary inspection by a border agent, the

² The facts related here are drawn from the record of the evidentiary hearing held before the magistrate judge.

Treasury Enforcement Communication System (“TECS”)³ returned a hit for Cotterman. The TECS hit indicated that Cotterman was a sex offender—he had a 1992 conviction for two counts of use of a minor in sexual conduct, two counts of lewd and lascivious conduct upon a child, and three counts of child molestation—and that he was potentially involved in child sex tourism. Because of the hit, Cotterman and his wife were referred to secondary inspection, where they were instructed to exit their vehicle and leave all their belongings in the car. The border agents called the contact person listed in the TECS entry and, following that conversation, believed the hit to reflect Cotterman’s involvement “in some type of child pornography.” The agents searched the vehicle and retrieved two laptop computers and three digital cameras. Officer Antonio Alvarado inspected the electronic devices and found what appeared to be family and other personal photos, along with several password-protected files.

Border agents contacted Group Supervisor Craig Brisbane at the Immigration and Customs Enforcement (“ICE”) office in Sells, Arizona, and informed him about Cotterman’s entry and the fact that he was a sex offender potentially involved in child sex tourism. The Sells Duty Agent, Mina Riley, also spoke with Officer Alvarado and then contacted the ICE Pacific Field Intelligence Unit, the office listed on the TECS hit, to get more information. That unit informed Riley that the alert was part of Operation Angel Watch, which was aimed at combating child sex tourism by identifying registered sex offenders in California, particularly those who travel frequently outside the United States. She was advised

³ The TECS is an investigative tool of the Department of Homeland Security that keeps track of individuals entering and exiting the country and of individuals involved in or suspected to be involved in crimes.

to review any media equipment, such as computers, cameras, or other electronic devices, for potential evidence of child pornography. Riley then spoke again to Alvarado, who told her that he had been able to review some of the photographs on the Cottermans' computers but had encountered password-protected files that he was unable to access.

Agents Brisbane and Riley departed Sells for Lukeville at about 1:30 p.m. and decided en route to detain the Cottermans' laptops for forensic examination. Upon their arrival, they gave Cotterman and his wife *Miranda* warnings and interviewed them separately. The interviews revealed nothing incriminating. During the interview, Cotterman offered to help the agents access his computer. The agents declined the offer out of concern that Cotterman might be able to delete files surreptitiously or that the laptop might be "booby trapped."

The agents allowed the Cottermans to leave the border crossing around 6 p.m., but retained the Cottermans' laptops and a digital camera.⁴ Agent Brisbane drove almost 170 miles from Lukeville to the ICE office in Tucson, Arizona, where he delivered both laptops and one of the three digital cameras to ICE Senior Special Agent & Computer Forensic Examiner John Owen. Agent Owen began his examination on Saturday, the following day. He used a forensic program to copy the hard drives of the electronic devices. He determined that the digital camera did not contain any contraband and released the camera that day to the Cottermans, who had traveled to Tucson from Lukeville and planned to stay there a few days. Agent Owen then used forensic software that often must run for several hours to examine copies of the laptop hard drives.

⁴ The other two cameras were returned to the Cottermans.

He began his personal examination of the laptops on Sunday. That evening, Agent Owen found seventy-five images of child pornography within the unallocated space of Cotterman's laptop.⁵

Agent Owen contacted the Cottermans on Sunday evening and told them he would need Howard Cotterman's assistance to access password-protected files he found on Cotterman's laptop. Cotterman agreed to provide the assistance the following day, but never showed up. When Agent Brisbine called again to request Cotterman's help in accessing the password-protected files, Cotterman responded that the computer had multiple users and that he would need to check with individuals at the company from which he had retired in order to get the passwords. The agents had no further contact with Cotterman, who boarded a flight to Mexico from Tucson the next day, April 9, and then flew onward to Sydney, Australia. On April 11, Agent Owen finally managed to open twenty-three password-protected files on Cotterman's laptop. The files revealed approximately 378 images of child pornography. The vast majority of the images were of the same girl, approximately 7–10 years of age, taken over a two- to three-year period. In many of the images, Cotterman was sexually molesting the child. Over the next few months, Agent Owen discovered hundreds more pornographic images, stories, and videos depicting children.

⁵ "Unallocated space is space on a hard drive that contains deleted data, usually emptied from the operating system's trash or recycle bin folder, that cannot be seen or accessed by the user without the use of forensic software. Such space is available to be written over to store new information." *United States v. Flyer*, 633 F.3d 911, 918 (9th Cir. 2011).

A grand jury indicted Cotterman for a host of offenses related to child pornography. Cotterman moved to suppress the evidence gathered from his laptop and the fruits of that evidence. The magistrate judge filed a Report and Recommendation finding that the forensic examination was an “extended border search” that required reasonable suspicion. He found that the TECS hit and the existence of password-protected files on Cotterman’s laptop were suspicious, but concluded that those facts did not suffice to give rise to reasonable suspicion of criminal activity. The district judge adopted the Report and Recommendation and granted Cotterman’s motion to suppress.

In its interlocutory appeal of that order, the government characterized the issue as follows: “Whether the authority to search a laptop computer *without reasonable suspicion* at a border point of entry permits law enforcement to take it to another location to be forensically examined, when it has remained in the continuous custody of the government.” A divided panel of this court answered that question in the affirmative and reversed. *United States v. Cotterman*, 637 F.3d 1068 (9th Cir. 2011). The panel concluded that reasonable suspicion was not required for the search and that “[t]he district court erred in suppressing the evidence lawfully obtained under border search authority.” *Id.* at 1084. In dissent, Judge Betty B. Fletcher wrote that “officers must have some level of particularized suspicion in order to conduct a seizure and search like the one at issue here.” *Id.* (B. Fletcher, J., dissenting). By a vote of a majority of nonrecused active judges, rehearing en banc was ordered. 673 F.3d 1206 (9th Cir. 2012). Following en banc oral argument, we requested supplemental briefing on the issue of whether reasonable suspicion existed at the time of the search.

II. WAIVER

The government argued below that the forensic examination was part of a routine border search not requiring heightened suspicion and, alternatively, that reasonable suspicion justified the search. Before the district court, the government maintained “the facts of this case clearly establish that there was reasonable suspicion.” However, having failed to obtain a favorable ruling on that ground, the government did not challenge on appeal the conclusion that there was no reasonable suspicion. Rather, it sought a broad ruling that no suspicion of any kind was required. Cotterman thus argued in his answering brief that the government had waived the issue—an assertion that the government did not address in its reply brief. Cotterman contends that the government has abandoned and conceded the issue of reasonable suspicion and that this court may not address that issue. We disagree.

We review de novo the ultimate question of whether a warrantless search was reasonable under the Fourth Amendment. *United States v. Johnson*, 256 F.3d 895, 905 (9th Cir. 2001) (en banc). Our review necessarily encompasses a determination as to the applicable standard: no suspicion, reasonable suspicion or probable cause. That the government may hope for the lowest standard does not alter our de novo review, particularly when the issue was fully briefed and argued below. Further, we may consider an issue that has not been adequately raised on appeal if such a failure will not prejudice the opposing party. *United States v. Ullah*, 976 F.2d 509, 514 (9th Cir. 1992). Where, as here, we “called for and received supplemental briefs by both parties,” *Alvarez v. INS*, 384 F.3d 1150, 1161 (9th Cir. 2004), the government’s failure to address the issue does not prejudice

Cotterman. *See also United States v. Resendiz-Ponce*, 549 U.S. 102, 103–04 (2007).

III. THE BORDER SEARCH

The broad contours of the scope of searches at our international borders are rooted in “the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country.” *Ramsey*, 431 U.S. at 616. Thus, border searches form “a narrow exception to the Fourth Amendment prohibition against warrantless searches without probable cause.” *Seljan*, 547 F.3d at 999 (internal quotation marks and citation omitted). Because “[t]he Government’s interest in preventing the entry of unwanted persons and effects is at its zenith at the international border,” *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004), border searches are generally deemed “reasonable simply by virtue of the fact that they occur at the border.” *Ramsey*, 431 U.S. at 616.

This does not mean, however, that at the border “anything goes.” *Seljan*, 547 F.3d at 1000. Even at the border, individual privacy rights are not abandoned but “[b]alanced against the sovereign’s interests.” *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985). That balance “is qualitatively different . . . than in the interior” and is “struck much more favorably to the Government.” *Id.* at 538, 540. Nonetheless, the touchstone of the Fourth Amendment analysis remains reasonableness. *Id.* at 538. The reasonableness of a search or seizure depends on the totality of the circumstances, including the scope and duration of the deprivation. *See United States v. Jacobsen*, 466 U.S. 109, 124 (1984); *see also United States v. Duncan*, 693 F.2d 971, 977 (9th Cir. 1982).

In view of these principles, the legitimacy of the initial search of Cotterman's electronic devices at the border is not in doubt. Officer Alvarado turned on the devices and opened and viewed image files while the Cottermans waited to enter the country. It was, in principle, akin to the search in *Seljan*, where we concluded that a suspicionless cursory scan of a package in international transit was not unreasonable. 547 F.3d at 1004. Similarly, we have approved a quick look and unintrusive search of laptops. *United States v. Arnold*, 533 F.3d 1003, 1009 (9th Cir. 2008) (holding border search reasonable where "CBP officers simply 'had [traveler] boot [the laptop] up, and looked at what [he] had inside.'") (second alteration in original).⁶ Had the search of Cotterman's laptop ended with Officer Alvarado, we would be inclined to conclude it was reasonable even without particularized suspicion. *See id.* But the search here transformed into something far different. The difficult question we confront is the reasonableness, without a warrant, of the forensic examination that comprehensively analyzed the hard drive of the computer.

A. The Forensic Examination Was Not An Extended Border Search

Cotterman urges us to treat the examination as an extended border search that requires particularized suspicion.

⁶ Although the *Arnold* decision expressed its conclusion in broad terms, stating that, "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border," *Arnold*, 533 F.3d at 1008, the facts do not support such an unbounded holding. As an en banc court, we narrow *Arnold* to approve only the relatively simple search at issue in that case, not to countenance suspicionless forensic examinations. The dissent's extensive reliance on *Arnold* is misplaced in the en banc environment.

Although the semantic moniker “extended border search” may at first blush seem applicable here, our jurisprudence does not support such a claim. We have “define[d] an extended border search as 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) (internal quotation marks and citations omitted). The key feature of an extended border search is that an individual can be assumed to have cleared the border and thus regained an expectation of privacy in accompanying belongings. *See United States v. Abbouchi*, 502 F.3d 850, 855 (9th Cir. 2007) (“Because the *delayed* nature of an extended border search . . . necessarily entails a greater level of intrusion on legitimate expectations of privacy than an ordinary border search, the government must justify an extended border search with reasonable suspicion that the search may uncover contraband or evidence of criminal activity.”) (internal quotation marks omitted) (emphasis added).

Cotterman’s case is different. Cotterman was stopped and searched at the border. Although he was allowed to depart the border inspection station after the initial search, some of his belongings, including his laptop, were not. The follow-on forensic examination was not an “extended border search.” A border search of a computer is not transformed into an extended border search simply because the device is transported and examined beyond the border.

To be sure, our case law has not always articulated the “extended border search” doctrine with optimal clarity. But the confusion has come in distinguishing between facts

describing a functional border search and those describing an extended border search, not in defining the standard for a search at the border. *See, e.g., United States v. Cardona*, 769 F.2d 625, 628 (9th Cir. 1985) (“We have recently recognized the difficulty of making sharp distinctions between searches at the functional equivalent of the border and extended border searches.”). The “functional equivalent” doctrine effectively extends the border search doctrine to all ports of entry, including airports. *See Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973). A routine customs search at the “functional equivalent” of the border is “analyzed as a border search” and requires neither probable cause nor reasonable suspicion. *Seljan*, 547 F.3d at 999. This case involves a search initiated at the actual border and does not encounter any of the difficulties surrounding identification of a “functional” border. As to the extended border search doctrine, we believe it is best confined to cases in which, after an apparent border crossing or functional entry, an attenuation in the time or the location of conducting a search reflects that the subject has regained an expectation of privacy.⁷

In his dissent, Judge Smith advocates applying the extended border search doctrine because the forensic examination occurred 170 miles from the border and days after Cotterman’s entry. Moving the laptop to a specialized

⁷ This characterization is consistent with how our circuit and others have articulated the doctrine. *See, e.g., United States v. Villasenor*, 608 F.3d 467, 471–72 (9th Cir. 2010); *United States v. Yang*, 286 F.3d 940, 945–46 (7th Cir. 2002); *United States v. Hyde*, 37 F.3d 116, 120 n.2 (3d Cir. 1994); *United States v. Santiago*, 837 F.2d 1545, 1548 (11th Cir. 1988); *United States v. Gaviria*, 805 F.2d 1108, 1112 (2d Cir. 1986); *United States v. Niver*, 689 F.2d 520, 526 (5th Cir. 1982); *United States v. Bilir*, 592 F.2d 735, 739–40 (4th Cir. 1979).

lab at a distant location might highlight that the search undertaken there was an extensive one, but it is not the dispositive factor here. Because Cotterman never regained possession of his laptop, the fact that the forensic examination occurred away from the border, in Tucson, did not heighten the interference with his privacy. Time and distance become relevant to determining whether there is an adequate nexus to a recent border crossing only after the subject or items searched have entered. *See Villasenor*, 608 F.3d at 471 (explaining that reasonableness of extended border search depends on “whether the totality of the surrounding circumstances, including the time and distance elapsed” establish that items to be searched have recently entered the country) (internal quotation marks omitted). Cotterman’s computer never cleared customs so entry was never effected. In short, the extended border search doctrine does not fit the search here.

B. Forensic Examination At The Border Requires Reasonable Suspicion

It is the comprehensive and intrusive nature of a forensic examination—not the location of the examination—that is the key factor triggering the requirement of reasonable suspicion here.⁸ *See Cotterman*, 637 F.3d at 1086–87 n.6 (B. Fletcher, J., dissenting) (recognizing that “[a] computer search in a forensic lab will *always* be equivalent to an *identical* search at the border. The duration of a computer search is not

⁸ The concurrence goes to great lengths to “refute any such notion” that location and duration contributed to our holding reasonable suspicion required here. Concurrence at 40–43. We see no reason for such an exegesis; our opinion is clear on the point that these factors are not at issue.

controlled by *where* the search is conducted. The duration of a computer search is controlled by what one is looking for and how one goes about searching for it.”) (emphasis in original). The search would have been every bit as intrusive had Agent Owen traveled to the border with his forensic equipment. Indeed, Agent Owen had a laptop with forensic software that he could have used to conduct an examination at the port of entry itself, although he testified it would have been a more time-consuming effort. To carry out the examination of Cotterman’s laptop, Agent Owen used computer forensic software to copy the hard drive and then analyze it in its entirety, including data that ostensibly had been deleted. This painstaking analysis is akin to reading a diary line by line looking for mention of criminal activity—plus looking at everything the writer may have erased.⁹

Notwithstanding a traveler’s diminished expectation of privacy at the border, the search is still measured against the Fourth Amendment’s reasonableness requirement, which considers the nature and scope of the search. Significantly, the Supreme Court has recognized that the “dignity and privacy interests of the person being searched” at the border will on occasion demand “some level of suspicion in the case of highly intrusive searches of the person.” *Flores-Montano*, 541 U.S. at 152. Likewise, the Court has explained that “some searches of property are so destructive,” “particularly offensive,” or overly intrusive in the manner in which they

⁹ Agent Owen used a software program called EnCase that exhibited the distinctive features of computer forensic examination. The program copied, analyzed, and preserved the data stored on the hard drive and gave the examiner access to far more data, including password-protected, hidden or encrypted, and deleted files, than a manual user could access.

are carried out as to require particularized suspicion. *Id.* at 152, 154 n.2, 155–56; *Montoya de Hernandez*, 473 U.S. at 541. The Court has never defined the precise dimensions of a reasonable border search, instead pointing to the necessity of a case-by-case analysis. As we have emphasized, “[r]easonableness, when used in the context of a border search, is incapable of comprehensive definition or of mechanical application.” *Duncan*, 693 F.2d at 977 (internal quotation marks and citation omitted).

Over the past 30-plus years, the Supreme Court has dealt with a handful of border cases in which it reaffirmed the border search exception while, at the same time, leaving open the question of when a “particularly offensive” search might fail the reasonableness test. The trail begins with *United States v. Ramsey*, where the Court reserved judgment on this question: “We do not decide whether, and under what circumstances, a border search might be deemed ‘unreasonable’ because of the particularly offensive manner in which it is carried out.” 431 U.S. at 618 n.13. Of note, the Court cited two cases, albeit non-border cases, as examples: *Kremen v. United States*, 353 U.S. 346, 347–48 (1957) (holding unconstitutional an exhaustive warrantless search of a cabin and seizure of its entire contents that were moved 200 miles away for examination) and *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 358 (1931) (condemning as “lawless invasion of the premises and a general exploratory search” a warrantless “unlimited search, ransacking the desk, safe, filing cases and other parts of [an] office”).

Less than ten years later, in 1985, the Court observed that it had “not previously decided what level of suspicion would justify a seizure of an incoming traveler for purposes other than a routine border search” and then went on to hold in the

context of an alimentary canal search that reasonable suspicion was required for “the detention of a traveler at the border, beyond the scope of a routine customs search and inspection.” *Montoya de Hernandez*, 473 U.S. at 540–41. The Court’s reference to “routine border search” was parsed in a later case, *Flores-Montano*, where the Court explained that “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,” and, more specifically, to the gas tank of a car. 541 U.S. at 152. Accordingly, the Court rejected a privacy claim vis-a-vis an automobile gas tank.

We are now presented with a case directly implicating substantial personal privacy interests. The private information individuals store on digital devices—their personal “papers” in the words of the Constitution—stands in stark contrast to the generic and impersonal contents of a gas tank. *See, e.g., United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (expressing “doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year”). We rest our analysis on the reasonableness of this search, paying particular heed to the nature of the electronic devices and the attendant expectation of privacy.

The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler’s luggage or automobile. That is no longer the case. Electronic devices are capable of storing warehouses full of information. The average 400-gigabyte laptop hard drive can store over 200 million pages—the

equivalent of five floors of a typical academic library. See Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005) (explaining that an 80 GB hard drive is equivalent to 40 million pages or one floor of an academic library); see also LexisNexis, *How Many Pages in a Gigabyte?*, http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf. Even a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage.¹⁰

The nature of the contents of electronic devices differs from that of luggage as well. Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails. This type of material implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their "papers." U.S. Const. amend. IV. The express listing of papers "reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the government." *Seljan*, 547 F.3d at 1014 (Kozinski, C.J., dissenting); see also *New York v. P.J. Video, Inc.*, 475 U.S. 868, 873 (1986). These records are expected to be kept

¹⁰ We are puzzled by the dissent's speculation about "how many gigabytes of storage [one must] buy to secure the guarantee that reasonable suspicion will be required before one's devices are searched." Dissent at 68. We discuss the typical storage capacity of electronic devices simply to highlight the features that generally distinguish them from traditional baggage. Indeed, we do not and need not determine whether Cotterman's laptop possessed unusually large or simply "average" capacity in order to resolve that the forensic examination of it required reasonable suspicion.

private and this expectation is “one that society is prepared to recognize as ‘reasonable.’” *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).¹¹

Electronic devices often retain sensitive and confidential information far beyond the perceived point of erasure, notably in the form of browsing histories and records of deleted files. This quality makes it impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel. A person’s digital life ought not be hijacked simply by crossing a border. When packing traditional luggage, one is accustomed to deciding what papers to take and what to leave behind. When carrying a laptop, tablet or other device, however, removing files unnecessary to an impending trip is an impractical solution given the volume and often intermingled nature of the files. It is also a time-consuming task that may not even effectively erase the files.

The present case illustrates this unique aspect of electronic data. Agents found incriminating files in the unallocated space of Cotterman’s laptop, the space where the computer stores files that the user ostensibly deleted and maintains other “deleted” files retrieved from web sites the user has visited. Notwithstanding the attempted erasure of material or the transient nature of a visit to a web site,

¹¹ The dissent’s discussion about Facebook and other platforms where the user voluntarily transmits personal data over the Internet, often oblivious to privacy issues, Dissent at 65–66, is a red herring. Of course, willful disclosure of electronic data, like disclosure of other material, undercuts an individual’s expectation of privacy. But there was no such disclosure here. Nor does the border search implicate such an affirmative disclosure.

computer forensic examination was able to restore the files. It is as if a search of a person's suitcase could reveal not only what the bag contained on the current trip, but everything it had ever carried.

With the ubiquity of cloud computing, the government's reach into private data becomes even more problematic.¹² In the "cloud," a user's data, including the same kind of highly sensitive data one would have in "papers" at home, is held on remote servers rather than on the device itself. The digital device is a conduit to retrieving information from the cloud, akin to the key to a safe deposit box. Notably, although the virtual "safe deposit box" does not itself cross the border, it may appear as a seamless part of the digital device when presented at the border. With access to the cloud through forensic examination, a traveler's cache is just a click away from the government.

As Justice Scalia wrote, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo*, 533 U.S. at 33–34. Technology has the dual and conflicting capability to decrease privacy and augment the expectation of privacy. While the thermal imaging device in *Kyllo* threatened to expose the hour at

¹² "The term 'cloud computing' is based on the industry usage of a cloud as a metaphor for the ethereal internet. . . . An external cloud platform is storage or software access that is essentially rented from (or outsourced to) a remote public cloud service provider, such as Amazon or Google. . . . By contrast, an internal or private cloud is a cluster of servers that is networked behind an individual or company's own firewall." David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L. Rev. 2205, 2216 (2009) (internal citations omitted).

which “the lady of the house” took her daily “sauna and bath,” *id.* at 38, digital devices allow us to carry the very papers we once stored at home.

The point is technology matters. The Department of Homeland Security has acknowledged as much in the context of international travelers:

Where someone may not feel that the inspection of a briefcase would raise significant privacy concerns because the volume of information to be searched is not great, that same person may feel that a search of their laptop increases the possibility of privacy risks due to the vast amount of information potentially available on electronic devices.

DHS, Privacy Impact Assessment for the Border Searches of Electronic Devices 2 (Aug. 25, 2009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf.

This is not to say that simply because electronic devices house sensitive, private information they are off limits at the border. The relevant inquiry, as always, is one of reasonableness. But that reasonableness determination must account for differences in property. *See Samson v. California*, 547 U.S. 843, 848 (2006) (“Under our general Fourth Amendment approach, *we examine the totality of the circumstances* to determine whether a search is reasonable”) (internal quotation marks, citation, and alterations omitted) (emphasis added). Unlike searches involving a reassembled gas tank, *Flores-Montano*, 541 U.S. at 150, or

small hole in the bed of a pickup truck, *United States v. Chaudhry*, 424 F.3d 1051, 1054 (9th Cir. 2005), which have minimal or no impact beyond the search itself—and little implication for an individual’s dignity and privacy interests—the exposure of confidential and personal information has permanence. It cannot be undone. Accordingly, the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property.

After their initial search at the border, customs agents made copies of the hard drives and performed forensic evaluations of the computers that took days to turn up contraband. It was essentially a computer strip search. 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. It is little comfort to assume that the government—for now—does not have the time or resources to seize and search the millions of devices that accompany the millions of travelers who cross our borders. It is the potential unfettered dragnet effect that is troublesome.

We recognize the important security concerns that prevail at the border. The government’s authority to protect the nation from contraband is well established and may be “heightened” by “national cris[e]s,” such as the smuggling of illicit narcotics, *Montoya de Hernandez*, 473 U.S. at 538, the current threat of international terrorism and future threats yet to take shape. But even in the face of heightened concerns, we must account for the Fourth Amendments rights of travelers. *Id.* at 539.

The effort to interdict child pornography is also a legitimate one. But legitimate concerns about child pornography do not justify unfettered crime-fighting searches or an unregulated assault on citizens' private information. Reasonable suspicion is a modest, workable standard that is already applied in the extended border search, *Terry* stop,¹³ and other contexts. Its application to the forensic examination here will not impede law enforcement's ability to monitor and secure our borders or to conduct appropriate searches of electronic devices.

Nor does applying this standard impede the deterrent effect of suspicionless searches, which the dissent contends is critical to thwarting savvy terrorists and other criminals. Dissent at 63. The Supreme Court has never endorsed the proposition that the goal of deterring illegal contraband at the border suffices to justify any manner of intrusive search. Rather, reasonableness remains the touchstone and the Court has expressed support for the deterrence value of suspicionless searches of a routine nature, such as vehicle checkpoints near the border. *See United States v. Martinez-Fuerte*, 428 U.S. 543, 556 (1976) (“We note here *only the substantiality of the public interest in the practice of routine stops* for inquiry at permanent checkpoints, a practice which the Government identifies as the most important of the traffic-checking operations.”) (emphasis added). In practical terms, suspicionless searches of the type approved in *Arnold* will continue; border officials will conduct further, forensic examinations where their suspicions are aroused by what they find or by other factors. Reasonable suspicion leaves ample room for agents to draw on their expertise and experience to pick up on subtle cues that criminal activity may be afoot.

¹³ *Terry v. Ohio*, 392 U.S. 1, 30 (1983).

See United States v. Tiong, 224 F.3d 1136, 1140 (9th Cir. 2000).¹⁴

We have confidence in the ability of law enforcement to distinguish a review of computer files from a forensic examination. We do not share the alarm expressed by the concurrence and the dissent that the standard we announce will prove unmanageable or give border agents a “Sophie’s choice” between thorough searches and *Bivens* actions. Concurrence at 48–49; Dissent at 65. Determining whether reasonable suspicion is required does not necessitate a “complex legal determination[]” to be made on a “moment-by-moment basis.” Dissent at 61. Rather, it requires that officers make a commonsense differentiation between a manual review of files on an electronic device and application of computer software to analyze a hard drive, and utilize the latter only when they possess a “particularized and objective

¹⁴ The greatest obstacle to ferreting out contraband at the border has always been the sheer number of international travelers. Any contention that national security will be critically hampered by stripping border agents of a critical law enforcement tool—suspicionless forensic examinations of electronics—is undermined by the fact that, as a matter of commonsense and resources, it is only when reasonable suspicion is aroused that such searches typically take place. *See, e.g., Chaudhry*, 424 F.3d at 1054 (B. Fletcher, J., concurring) (“As a practical matter, border agents are too busy to do extensive searches (removing gas tanks and door panels, boring holes in truck beds) unless they have suspicion.”). As Judge Callahan acknowledges in her separate opinion, the record suggests that “remote and/or intensive searches of electronic devices crossing the border do not occur all that often.” Concurrence at 50 n.11. The reference that only a small fraction of travelers at the border have their devices searched simply reinforces our point—our ruling will not place an undue burden on border agents who already rely on a degree of suspicion in referring travelers to secondary inspection.

basis for suspecting the person stopped of criminal activity.” *Tiong*, 224 F.3d at 1140 (internal quotation marks omitted).

International travelers certainly expect that their property will be searched at the border. What they do not expect is that, absent some particularized suspicion, agents will mine every last piece of data on their devices or deprive them of their most personal property for days (or perhaps weeks or even months, depending on how long the search takes). *United States v. Ramos-Saenz*, 36 F.3d 59, 61 n.3 (9th Cir. 1994) (“Intrusiveness includes both the extent of a search as well as the degree of indignity that may accompany a search.”). Such a thorough and detailed search of the most intimate details of one’s life is a substantial intrusion upon personal privacy and dignity. We therefore hold that the forensic examination of Cotterman’s computer required a showing of reasonable suspicion, a modest requirement in light of the Fourth Amendment.

IV. REASONABLE SUSPICION

Reasonable suspicion is defined as “a particularized and objective basis for suspecting the particular person stopped of criminal activity.” *United States v. Cortez*, 449 U.S. 411, 417–18 (1981). This assessment is to be made in light of “the totality of the circumstances.” *Id.* at 417. “[E]ven when factors considered in isolation from each other are susceptible to an innocent explanation, they may collectively amount to a reasonable suspicion.” *United States v. Berber-Tinoco*, 510 F.3d 1083, 1087 (9th Cir. 2007). We review reasonable suspicion determinations de novo, reviewing findings of historical fact for clear error and giving “due weight to inferences drawn from those facts by resident judges and

local law enforcement officers.” *Ornelas v. United States*, 517 U.S. 690, 699 (1996).

In the district court and in supplemental briefing, the government argued that the border agents had reasonable suspicion to conduct the initial search and the forensic examination of Cotterman’s computer. We agree.

The objective facts reflect that both the agents at the border and the agents who arrived later from Sells based their decision to search Cotterman’s belongings on the TECS hit. Officer Alvarado was told by those in charge of administering the TECS database that he should search Cotterman’s property because the TECS hit indicated “that [Cotterman] appeared to [have] been involved in some type of child pornography.” Agent Riley also looked up Cotterman’s criminal record and understood that he had a prior conviction for child pornography. As it turned out, Cotterman’s previous conviction was not for pornography, but for child molestation. Nonetheless, the agents’ *understanding* of the objective facts, albeit mistaken, is the baseline for determining reasonable suspicion. See *Liberal v. Estrada*, 632 F.3d 1064, 1077 (9th Cir. 2011) (“Even if an officer makes a mistake of fact, that mistake ‘will not render a stop illegal, if the objective facts known to the officer gave rise to a reasonable suspicion that criminal activity was afoot.’” (quoting *United States v. Mariscal*, 285 F.3d 1127, 1131 (9th Cir. 2002))).

By itself, Cotterman’s 1992 conviction for child molestation does not support reasonable suspicion to conduct an extensive forensic search of his electronic devices. “Although a prior criminal history cannot alone establish reasonable suspicion . . . it is permissible to consider such a

fact as part of the total calculus of information in th[at] determination[.]” *Burrell v. McIlroy*, 464 F.3d 853, 858 n.3 (9th Cir. 2006). The TECS alert was not based merely on Cotterman’s conviction—the agents were aware that the alert targeted Cotterman because he was a sex offender “who travel[ed] frequently out of the country” and who was “possibly involved in child sex tourism.” Further, Agent Riley testified that an examination of Cotterman’s passport confirmed that he had traveled in and out of the country frequently since his conviction in 1992.

In further support of reasonable suspicion, the government asserts that Mexico, from which the Cottermans were returning, is “a country associated with sex tourism.”¹⁵ The ICE field office specifically informed Agent Riley that the alert was part of Operation Angel Watch, which targeted individuals potentially involved in sex tourism and alerted officials to be on the lookout for laptops, cameras and other paraphernalia of child pornography. *See* 156 Cong. Rec. S9581-03 (daily ed. Dec. 14, 2010) (describing Operation Angel Watch as a program “help[ing] ICE [to] identify travel patterns of convicted sex offenders who may attempt to exploit children in foreign countries”). Cotterman’s TECS alert, prior child-related conviction, frequent travels, crossing from a country known for sex tourism, and collection of electronic equipment, plus the parameters of the Operation

¹⁵ It is ironic that the dissent expresses concern that, by factoring in the incidence of crime in particular countries, “thousands of individuals . . . will now be forced to reconsider traveling to entire countries . . . or will need to leave all their electronic equipment behind, to avoid arousing a ‘reasonable’ suspicion,” Dissent at 78, when, if forensic examination of those travelers’ electronics occurs at the border, the dissent would require *no suspicion at all*.

Angel Watch program, taken collectively, gave rise to reasonable suspicion of criminal activity.

To these factors, the government adds another—the existence of password-protected files on Cotterman’s computer.¹⁶ We are reluctant to place much weight on this factor because it is commonplace for business travelers, casual computer users, students and others to password protect their files. Law enforcement “cannot rely solely on factors that would apply to many law-abiding citizens,” *Berber-Tinoco*, 510 F.3d at 1087, and password protection is ubiquitous. National standards require that users of mobile electronic devices password protect their files. *See generally* United States Department of Commerce, Computer Security Division, National Institute of Standards and Technology, Computer Security (2007) (NIST Special Publication 800-111). Computer users are routinely advised—and in some cases, required by employers—to protect their files when traveling overseas. *See, e.g.*, Michael Price, *National Security Watch*, 34-MAR Champion 51, 52 (March 2010) (“[T]here is one relatively simple thing attorneys can do [when crossing the border] to protect their privacy and the rights of their clients: password-protect the computer login and any sensitive files or folders.”).

Although password protection of files, in isolation, will not give rise to reasonable suspicion, where, as here, there are other indicia of criminal activity, password protection of files

¹⁶ Agent Riley testified that Alvarado told her that he had “encounter[ed] some *files* that were password protected,” while Agent Alvarado testified that he found one file.

may be considered in the totality of the circumstances.¹⁷ To contribute to reasonable suspicion, encryption or password protection of files must have some relationship to the suspected criminal activity. Here, making illegal files difficult to access makes perfect sense for a suspected holder of child pornography. When combined with the other circumstances, the fact that Officer Alvarado encountered at least one password protected file on Cotterman's computer contributed to the basis for reasonable suspicion to conduct a forensic examination.

The existence of the password-protected files is also relevant to assessing the reasonableness of the scope and duration of the search of Cotterman's computer. The search was necessarily protracted because of the password protection that Cotterman employed. After Cotterman failed to provide agents with the passwords to the protected files and fled the country, it took Agent Owen days to override the computer security and open the image files of child pornography.

Although we must take into account factors weighing both in favor and against reasonable suspicion, Cotterman's innocent explanation does not tip the balance. *See Tiong*, 224 F.3d at 1140 (recognizing that "innocent possibilities . . . do not undermine reasonable suspicion"). The dissent suggests that Cotterman's offer at the border "to help the agents access his computer" counsels against a finding of reasonable suspicion. Dissent at 80. The agents were

¹⁷ We do not suggest that password protecting an entire device—as opposed to files within a device—can be a factor supporting a reasonable suspicion determination. Using a password on a device is a basic means of ensuring that the device cannot be accessed by another in the event it is lost or stolen.

appropriately wary of such an offer due to concerns that Cotterman could tamper with the devices. Nor did the agents' discovery of vacation photos eliminate the suspicion that Cotterman had engaged in criminal activity while abroad or might be importing child pornography into the country. Because the first examination of Cotterman's laptop, by Officer Alvarado, turned up nothing incriminating, Cotterman urges that any suspicion prompted by the TECS alert was dispelled by this initial failure. But the nature of the alert on Cotterman, directing agents to review media and electronic equipment for child pornography, justified conducting the forensic examination despite the failure of the first search to yield any contraband.

Collectors of child pornography can hardly be expected to clearly label such files and leave them in readily visible and accessible sections of a computer's hard drive, particularly when they are traveling through border crossings, where individuals ordinarily anticipate confronting at least a cursory inspection. Officer Alvarado, who was responsible for conducting the initial search, was specifically looking for photographs as described in the TECS hit but testified that he had only a slightly above-average familiarity with laptops. He could do no more than open a file, look at it and see if he could access it. He testified that "[i]f [he] encountered something that [he] could not access, then [he] would reference it to somebody that may have that ability to look at [it]." That is precisely what occurred here. Officer Alvarado came across password-protected files but, unable to open them, moved on to other files. Alvarado told Agent Riley about the password protection, and she and Agent Brisbine decided to seize the computers for further examination. The border agents "certainly had more than an inchoate and unparticularized suspicion or hunch" of criminal activity to

support their decision to more carefully search for evidence of child pornography. *Montoya de Hernandez*, 473 U.S. at 542 (internal quotation marks and citation omitted). An alert regarding possession of this type of criminal contraband justified obtaining additional resources, here available in Tucson, to properly determine whether illegal files were present.

Unlike the dissent, we credit the agents' observations and experience in acting upon significant myriad factors that support reasonable suspicion. It is not our province to nitpick the factors in isolation but instead to view them in the totality of the circumstances. For the above reasons, we conclude that the examination of Cotterman's electronic devices was supported by reasonable suspicion and that the scope and manner of the search were reasonable under the Fourth Amendment. Cotterman's motion to suppress therefore was erroneously granted.

REVERSED.

CALLAHAN, Circuit Judge, concurring in part, dissenting in part, and concurring in the judgment, with whom CLIFTON, Circuit Judge, joins, and with whom M. SMITH, Circuit Judge, joins as to all but Part II.A:

Whether it is drugs, bombs, or child pornography, we charge our government with finding and excluding any and all illegal and unwanted articles and people before they cross our international borders. Accomplishing that Herculean task requires that the government be mostly free from the Fourth Amendment's usual restraints on searches of people and their

property. Today the majority ignores that reality by erecting a new rule requiring reasonable suspicion for any thorough search of electronic devices entering the United States. This rule flouts more than a century of Supreme Court precedent, is unworkable and unnecessary, and will severely hamstring the government's ability to protect our borders.

I therefore dissent from Part III of the majority's opinion. I concur in Parts I, II, and IV, and in particular the majority's conclusion in Part IV that the government had reasonable suspicion to conduct the forensic examination of Howard Cotterman's electronic devices. I therefore also concur in the judgment.

I.

Over the last 125 years, the Supreme Court has explained that the United States and its people have a "paramount interest" in national self-protection and an "inherent" right to exclude illegal and "unwanted persons and effects." *United States v. Flores-Montano*, 541 U.S. 149, 152–53 (2004); see also *United States v. Montoya de Hernandez*, 473 U.S. 531, 537–40 (1985); *United States v. Ramsey*, 431 U.S. 606, 616–18 (1977); *United States v. Thirty-Seven (37) Photographs*, 402 U.S. 363, 376 (1971); *Carroll v. United States*, 267 U.S. 132, 154 (1925); *Boyd v. United States*, 116 U.S. 616, 623 (1886). Accordingly, "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Flores-Montano*, 541 U.S. at 152.

To effectuate this interest, the Supreme Court has recognized a broad exception to the Fourth Amendment's requirement of probable cause or a warrant for searches

conducted at the border. Under that exception, searches of people and their property at the United States borders and their functional equivalents are *per se* reasonable, meaning that they typically do not require a warrant, probable cause, or even reasonable suspicion. *Montoya de Hernandez*, 473 U.S. at 538; *see also Flores-Montano*, 541 U.S. at 152–53; *Ramsey*, 431 U.S. at 616–18; *United States v. Seljan*, 547 F.3d 993, 999–1000 (9th Cir. 2008) (en banc), *cert. denied*, 129 S. Ct. 1368 (2009).

In the long time that the Court has recognized the border search doctrine, the Court has found just *one* search at the border that required reasonable suspicion. *See Montoya de Hernandez*, 473 U.S. at 541 (upholding the 24-hour detention of a woman suspected of smuggling illegal drugs in her digestive system, followed by a pregnancy test and rectal examination, based on reasonable suspicion). In the remaining cases, the Court consistently has described the government’s border search authority in very broad terms¹

¹ *See, e.g., Flores-Montano*, 541 U.S. at 152 (“The Government’s interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.”); *id.* at 153 (“It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity.”); *Ramsey*, 431 U.S. at 617 (“This interpretation, that border searches were not subject to the warrant provisions of the Fourth Amendment and were ‘reasonable’ within the meaning of that Amendment, has been faithfully adhered to by this Court.”); *id.* at 620 (“The border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country.”); *Thirty-Seven (37) Photographs*, 402 U.S. at 376 (“[A traveler’s] right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during such a search. Customs officers characteristically inspect luggage and their power to do so is not

and overturned the lower courts' attempts to cabin that authority.² The Court also repeatedly has gone out of its way to explain that border searches generally are exempt from the limits it imposes on domestic searches. *See, e.g., Flores-Montano*, 541 U.S. at 154 (“[O]n many occasions, we have noted that the expectation of privacy is less at the border than it is in the interior.”); *Montoya de Hernandez*, 473 U.S. at 539–40 (“But not only is the expectation of privacy less at the border than in the interior, the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border.” (internal and external citations omitted)); *United States v. 12 200-Foot Reels of Super 8mm. Film*, 413 U.S. 123, 125 (1973) (“Import restrictions and searches of persons or packages at the national borders rest on

questioned in this case; it is an old practice and is intimately associated with excluding illegal articles from the country.”); *Carroll*, 267 U.S. at 154 (“Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in.”). Even in *Montoya de Hernandez* the Court described the government’s border search authority expansively. *See* 473 U.S. at 539–40, 542–44.

² *See, e.g., Flores-Montano*, 541 U.S. at 152–55 (overturning the Ninth Circuit’s conclusion that the border search of a gas tank required reasonable suspicion); *Ramsey*, 431 U.S. at 616–22 (overturning the D.C. Circuit’s conclusion that the search of international mail required probable cause); *Thirty-Seven (37) Photographs*, 402 U.S. at 376 (relying in part on border search doctrine to overturn lower court’s decision that statute barring the importation of obscene material was unconstitutional).

different considerations and different rules of constitutional law from domestic regulations.”).³

II.

It is against this legal backdrop that we must assess the constitutionality of the government’s search in this case. As with all searches subject to Fourth Amendment review, the constitutionality of a border search turns on whether it is reasonable. *See Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006) (“[T]he ultimate touchstone of the Fourth Amendment is ‘reasonableness.’”). Under the border search doctrine, suspicionless border searches are *per se* reasonable. However, the Supreme Court has identified three situations in which they might not be *per se* reasonable, *i.e.*, at least reasonable suspicion is required: (1) “highly intrusive searches of the person;” (2) destructive searches of property;

³ *See also City of Indianapolis v. Edmond*, 531 U.S. 32, 47–48 (2000) (explaining that decision barring domestic drug interdiction checkpoints “does not affect the validity of border searches or searches at places like airports”); *United States v. Ross*, 456 U.S. 798, 823 (1982) (explaining that while the Fourth Amendment gives protection to containers in domestic vehicles, “[t]he luggage carried by a traveler entering the country may be searched at random by a customs officer”); *Torres v. Puerto Rico*, 442 U.S. 465, 472–74 (1979) (distinguishing between United States–Puerto Rico border and international borders in holding unconstitutional the search of a traveler’s luggage without “articulable suspicion”); *United States v. Brignoni-Ponce*, 422 U.S. 873, 884 (1975) (“Except at the border and its functional equivalents, officers on roving patrol may stop vehicles” only with reasonable suspicion they contain illegal aliens); *Almeida-Sanchez v. United States*, 413 U.S. 266, 272–76 (1973) (distinguishing searches of vehicles at the border from a search that occurred 25 miles away); *Carroll*, 267 U.S. at 151–54 (distinguishing between interior and border searches of vehicles and persons).

and (3) searches conducted in a “particularly offensive” manner. *Flores-Montano*, 541 U.S. at 152–56 & n.2.

Although its opinion is not entirely clear, the majority appears to rely on the first and third exceptions to hold that the search at issue in this case required reasonable suspicion. (There is no claim that the government damaged or destroyed Cotterman’s property.) But the exception for “highly intrusive searches of the person,” *Flores-Montano*, 541 U.S. at 152, cannot apply here; “papers,” even private ones in electronic format, are not a “person.” *See id.* (“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.”). That leaves the exception for searches conducted in a “particularly offensive” manner. *Id.* at 154 n.2. The majority relies primarily on the notion that electronic devices are special to conclude that reasonable suspicion was required. Majority at 20–28. The majority is mistaken.

A.

The majority correctly concludes that the government’s forensic search in Tucson was not an extended border search, as the border agents retained custody of Cotterman’s laptop.⁴

⁴ I agree with the majority that this case does not involve an extended border search. Unlike a border search, an extended border search takes place at a location “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) (internal quotation marks and citation omitted), *cert. denied*, 131 S. Ct. 67 (2010). Reasonable suspicion is required precisely because the individual

Id. at 9, 14–15. The majority also states that “[i]t is the comprehensive and intrusive nature of a forensic examination—not the location of the examination—that is the key factor triggering the requirement of reasonable suspicion here.” Majority at 17. The inclusion of the word “key” might be read to imply that some other factor, such as the location and duration of the search, contributed to its purported unreasonableness. I write to refute any such notion.

First consider the facts. The border agents took Cotterman’s electronic devices to the nearest computing center (to Tucson, where Cotterman and his wife were already traveling), before clearing them for entry into the United States. The computer specialist moved the search ahead of his other work and conducted it over the weekend. Although the forensic search lasted five days, it took only 48 hours to discover the initial 75 images of child pornography. The agents were reasonably reluctant to rely on Cotterman’s offer to help, since he might have deleted or otherwise made unrecoverable any contraband that his devices contained. The agents returned the devices as soon as they cleared them.

has regained an expectation of privacy by moving away from the border. *See United States v. Villasenor*, 608 F.3d 467, 471–72 (9th Cir.), *cert. denied*, 131 S. Ct. 547 (2010); *United States v. Whiting*, 781 F.2d 692, 695 (9th Cir. 1986). Here, there was no attenuation between Cotterman’s border crossing and the forensic search of his electronic property; the government conducted that search *before* clearing the property for entry and *before* Cotterman could regain an expectation of privacy in that property. *See* 19 U.S.C. § 1499 (providing that imported goods are permitted entry only after Customs clears them); *United States v. Alfonso*, 759 F.2d 728, 734 (9th Cir. 1985) (“Extended border searches occur after the actual entry has been effected and intrude more on an individual’s normal expectation of privacy.”).

Now consider the law. The Supreme Court has upheld the constitutionality of a police search of packages retrieved from an automobile, even though the police conducted their search three days after the police stopped the vehicle and at the police station. *United States v. Johns*, 469 U.S. 478, 485–88 (1985). The Court rejected the argument that “searches of containers discovered in the course of a vehicle search are subject to temporal restrictions not applicable to the vehicle search itself.” *Id.* at 485. Although *Johns* involved a domestic automobile search based on probable cause, it still stands for the proposition, equally applicable to this case, that “the legality of the search was determined by reference to the [applicable] exception to the warrant requirement.” *Id.*

In the border search context, the Supreme Court, in upholding the lengthy detention of a person reasonably suspected of smuggling drugs in her digestive system at an airport, addressed whether that detention was “reasonably related in scope to the circumstances which justified it initially.” *Montoya de Hernandez*, 473 U.S. at 542. The Court explained that: (1) “courts should not indulge in unrealistic second-guessing” when answering this question, as “[a]uthorities must be allowed to graduate their response to the demands of any particular situation;” (2) the Court consistently has “refused to charge police with delays in investigatory detention attributable to the suspect’s evasive actions;” and (3) “we have also consistently rejected hard-and-fast time limits.” *Id.* at 542–43 (quotation marks and citations omitted). The Court emphasized that, at the international border, “the Fourth Amendment balance of interests leans heavily to the Government” because the government is charged not just with investigating crime but with “protecting this Nation from entrants who may bring anything harmful into this country.” *Id.* at 544. Finally, any

“length” or “discomfort” associated with a border search does not offend the Fourth Amendment when it “result[s] solely from the method by which [a traveler] cho[oses] to smuggle [contraband] into this country.” *Id.*

Any suggestion that the government’s search here was “particularly offensive” due to the location and duration of the search runs counter to the Supreme Court’s admonitions in *Johns* and *Montoya de Hernandez*. It also effectively requires the government to supply every port of entry with the equipment and staff needed to conduct forensic electronic searches, or at least to have such equipment and staff waiting at a nearby location. Such a requirement is unreasonable, particularly since the record in this case suggests that a forensic search of Cotterman’s electronic devices at the border station would have taken *longer* than the search at the Tucson computing center.⁵ See *United States v. Hill*, 459 F.3d 966, 974–75 (9th Cir. 2006), *cert. denied*, 127 S. Ct. 1863 (2007) (discussing problems inherent in requiring police to bring with them equipment to search electronic media); *cf.* *Johns*, 469 U.S. at 486–87 (explaining that requiring police

⁵ The district court found that the government could have conducted the forensic search at the Lukeville border station. *United States v. Cotterman*, No. CR 07-1207-TUC-RCC, 2009 WL 465028, at *1 (D. Ariz. Feb. 24, 2009). The court presumably based this finding on testimony that the computer specialist who conducted the forensic examination had a specially-equipped laptop. However, the specialist testified that using his laptop at the border station, rather than transporting Cotterman’s electronic devices to the Tucson computer center, would have taken “a lot longer” because the laptop was “not nearly as extensive as what I have in my lab,” the “processor in my laptop is much slower” than the lab equipment, and “I could only do one computer at a time with the laptop.” Technical difficulties also could have slowed down an examination conducted at the border station.

officers to immediately inspect all packages “would be of little benefit to the person whose property is searched”).

B.

The majority’s opinion turns primarily on the notion that electronic devices deserve special consideration because they are ubiquitous and can store vast quantities of personal information. That idea is fallacious and has no place in the border search context.

The Supreme Court has been willing to distinguish only between border searches of people and property, not between different types of property. In 2004, in *Flores-Montano*, the Court explained that

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. Complex balancing tests to determine what is a “routine” search of a vehicle, as opposed to a more “intrusive” search of a person, have no place in border searches of vehicles.

541 U.S. at 152. We have since applied *Flores-Montano* to hold that any distinction between “routine” and “nonroutine” searches does not apply to searches of property, and that there can be no “least restrictive means” test for border searches. *United States v. Chaudhry*, 424 F.3d 1051, 1054 (9th Cir. 2005), *cert. denied*, 547 U.S. 1083 (2006); *United States v. Cortez-Rocha*, 394 F.3d 1115, 1122–23 (9th Cir. 2004), *cert.*

denied, 546 U.S. 849 (2005).⁶ Put another way, the Supreme Court—and, reluctantly, this court—have refused to adopt a sliding “intrusiveness” scale for border searches of property. Thus, the Court has all but held that property that crosses the border, whatever it is, does not merit Fourth Amendment protection.

Of course, *Flores-Montano*, *Chaudhry*, and *Cortez-Rocha* involved vehicles or parts of vehicles, not electronic devices, and the other border search cases that have reached the Supreme Court all involved containers of some sort. *See, e.g., Ramsey*, 431 U.S. at 616–22 (mail); *Thirty-Seven (37) Photographs*, 402 U.S. at 376 (luggage). And yes, the Court has left open the possibility that a border search might be “‘unreasonable’ because of the particularly offensive manner in which it is carried out.” *Flores-Montano*, 541 U.S. at 154 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13). But is the mere fact that Cotterman chose to save his child pornography electronically, rather than print it out on paper, enough to invoke that exception?

The two courts of appeals—including this court—that have had occasion to address whether electronic devices

⁶ In 1985, the Supreme Court wrote about the government’s “plenary authority to conduct *routine* searches and seizures at the border.” *Montoya de Hernandez*, 473 U.S. at 537 (emphasis added); *see also id.* at 541 n.4 (“Because the issues are not presented today we suggest no view on what level of suspicion, if any, is required for *nonroutine* border searches such as strip, body-cavity, or involuntary x-ray searches.”) (emphasis added). We unfortunately seized on the word “routine” to establish a sliding scale of intrusiveness, with more intrusive (*i.e.*, less “routine”) searches requiring reasonable suspicion. *See, e.g., United States v. Molina-Tarazon*, 279 F.3d 709, 711–13 (9th Cir. 2002). *Flores-Montano* plainly repudiated that approach.

deserve special consideration have correctly concluded that they do not. In *United States v. Arnold*, 533 F.3d 1003, 1008–10 (9th Cir. 2008), *cert. denied*, 555 U.S. 1176 (2009), we held that laptops are like other property, relying on the reasoning and language in *Flores-Montano*, *Chaudhry*, and *Cortez-Rocha* discussed above (among other cases). Similarly, in *United States v. Ickes*, 393 F.3d 501, 503–07 (4th Cir. 2005), the Fourth Circuit upheld an extensive border search of the defendant’s laptop that revealed child pornography. Notably, the court held that the border agents had reasonable suspicion to search the defendant’s laptop, but explained why that did not matter:

The agents did not inspect the contents of Ickes’s computer until they had already discovered marijuana paraphernalia, photo albums of child pornography, a disturbing video focused on a young ball boy, and an outstanding warrant for Ickes’s arrest. As a practical matter, computer searches are most likely to occur where—as here—the traveler’s conduct or the presence of other items in his possession suggest the need to search further. However, to state the probability that reasonable suspicions will give rise to more intrusive searches is a far cry from enthroneing this notion as a matter of constitutional law. The essence of border search doctrine is a reliance upon the trained observations and judgments of customs officials, rather than upon constitutional requirements applied to the inapposite context of this sort of search.

Id. at 507. Thus, the Fourth Circuit has recognized what the majority does not: electronic devices are like any other container that the Supreme Court has held may be searched at the border without reasonable suspicion.⁷ Though we are not bound by *Arnold* nor *Ickes* in this en banc proceeding, we *are* bound by what the Supreme Court has said: in the unique context of border searches, property is property and we may not chip away at the government’s authority to search it by adopting a sliding scale of intrusiveness. It’s the border, not the technology, that “matters.” Majority at 24; *cf. Ramsey*, 431 U.S. at 620 (“It is clear that there is nothing in the rationale behind the border-search exception which suggests that the mode of entry will be critical.”).

Logic and commonsense, not just Supreme Court precedent, reveal the flaws in the majority’s opinion. The fact that electronic devices are capable of storing a lot of personal information does not make an extensive search of them “particularly offensive.” We have squarely rejected the idea that the “intrusiveness” of a search depends in whole or in part on the nature of the property being searched. In *United States v. Giberson*, 527 F.3d 882 (9th Cir. 2008), we specifically rebuffed the argument that computers are special for Fourth Amendment purposes by virtue of how much information they store; “neither the quantity of information, nor the form in which it is stored, is legally relevant in the Fourth Amendment context.” *Id.* at 888; *see also California v. Carney*, 471 U.S. 386, 393–94 (1985) (rejecting applying

⁷ I agree with Judge Smith that the majority’s opinion appears to create an imprudent split with the Fourth Circuit. *See* Dissent at 58.

Fourth Amendment protection to property (a mobile home) that is “capable of functioning as a home” simply on account of the property’s size or “worth[iness]” as a container); *United States v. Payton*, 573 F.3d 859, 864 (9th Cir. 2009) (“*Giberson* held that computers were not entitled to a special categorical protection of the Fourth Amendment.”); *Kyllo v. United States*, 533 U.S. 27, 41 (2001) (Stevens, J., dissenting) (explaining that Fourth Amendment exceptions and distinctions based solely on a type of technology are “unwise[] and inconsistent with the Fourth Amendment”).

While *Giberson* and *Carney* involved domestic searches, their reasoning applies equally in the border search context. If the government may search the contents of a briefcase, car, or mobile home that transits the border, there is no reason it should not also be able to search the contents of a camera, tablet, or laptop that enters the country. All of those things are capable of storing, and often do store, private information. See *Ross*, 456 U.S. at 823 (“The luggage carried by a traveler entering the country may be searched at random by a customs officer; *the luggage may be searched no matter how great the traveler’s desire to conceal the contents may be.*” (emphasis added)). The majority points out that electronic devices can and usually do store much *more* private information than their non-electronic counterparts. Majority at 17–24. But “a port of entry is not a traveler’s home,” *Thirty-Seven (37) Photographs*, 402 U.S. at 376, even if a traveler chooses to carry a home’s worth of personal information across it.⁸

⁸ The element of choice is crucial. The fact that border searches occur at fixed times and checkpoints makes them inherently less intrusive; a person “with advance notice of the location of a permanent checkpoint has an opportunity to avoid the search entirely, or at least to prepare for, and limit, the intrusion on her privacy.” *Mich. Dep’t of State Police v. Sitz*,

Moreover, a bright-line rule distinguishing electronic from non-electronic devices—of the sort the Supreme Court has made clear has no place in Fourth Amendment jurisprudence, *Ohio v. Robinette*, 519 U.S. 33, 39 (1996)—is arbitrary; there is no reason someone carrying a laptop should receive greater privacy protection than someone who chooses (or can only afford) to convey his or her personal information on paper.

In short, today the court erects a new bright-line rule: “forensic examination” of electronic devices “at the border requires reasonable suspicion.” Majority at 17; *see also id.* at 21 n.10. The majority never defines “forensic,” leaving border agents to wonder exactly what types of searches are

496 U.S. 444, 463 (1990) (Stevens, J., dissenting); *see also Montoya de Hernandez*, 473 U.S. at 544 (“Respondent’s detention was long, uncomfortable, indeed, humiliating; but both its length and its discomfort resulted solely from the method by which she chose to smuggle illicit drugs into this country.”).

The element of choice goes to the more fundamental issue of whether someone can have any reasonable expectation of privacy when he or she voluntarily carries electronic equipment across the border. Border officers are permitted to examine a written diary, and someone who wants to keep the contents of a diary secret should know not to take it across the border. The same should be true for personal data stored on a laptop or other electronic device rather than a written diary.

Moreover, the fact that the Fourth Amendment does not apply in foreign countries further weakens any claim to a reasonable expectation of privacy in property that crosses the United States border. Carrying an electronic device outside the United States almost always entails carrying it into another country, making it subject to search under that country’s laws. Travelers expect these intrusions, or at least their possibility.

off-limits.⁹ Even if the majority means to require reasonable suspicion for *any* type of digital forensic border search, no court has ever erected so categorical a rule, based on so general a type of search or category of property, and the Supreme Court has rightly slapped down anything remotely similar. The majority invites—indeed, requires—the Court to do so again.¹⁰

III.

The majority's holding contravenes Supreme Court precedent, defies logic and commonsense, and is unworkable. It is also unnecessary and will impair the federal government's ability to protect our borders.

As Judge Smith points out in his dissent, “[b]order patrol agents process hundreds of thousands of travelers each day and conduct thousands of searches on electronic devices each year.” Dissent at 61–62 (citation omitted). All the evidence in this case suggests that the government does not have the resources—time, personnel, facilities, or technology—to exhaustively search every (or even a majority) of the electronic devices that cross our borders. *Cf. Ickes*, 393 F.3d at 507. Unless we somehow manage to solve our fiscal problems, and unless the government somehow manages to

⁹ See Darrin J. Behr, *Anti-Forensics: What it Does and Why You Need to Know*, 255 N.J. Law. 9, 10 (Dec. 2008) (“Due to the fact that there are hundreds of digital forensic investigation procedures developed all over the world, digital forensics has yet to be defined.”).

¹⁰ I note that a case currently pending in the Sixth Circuit appears to raise similar issues as this case. See *United States v. Stewart*, No. 12-1427 (6th Cir. filed Apr. 5, 2012); see also *United States v. Stewart*, 715 F. Supp. 2d 750 (E.D. Mich. 2010).

acquire better technology at a faster pace than the rest of us, these restraints will continue. That means border agents must prioritize who, what, and how they search. By and large, border agents will conduct forensic electronic searches of people who, like Howard Cotterman, the agents reasonably suspect may be trying to carry illegal articles into, or themselves illegally enter, the country.¹¹ That agents typically will have reasonable suspicion is, of course, “a far cry from enthroneing this notion as a matter of constitutional law.” *Ickes*, 393 F.3d at 507.

The majority finds this reality check to be of “little comfort[;] [i]t is the potential unfettered dragnet effect that is troublesome.” Majority at 25. But that abstract risk, which exists with any exception to the Fourth Amendment, does not justify a bright-line rule requiring reasonable suspicion for any thorough search of electronic devices entering the United

¹¹ Testimony from the suppression hearing in this case suggests that remote and/or intensive searches of electronic devices crossing the border do not occur all that often. For example, the computer specialist who conducted the forensic search of Cotterman’s laptop testified that the search was the first one he was asked to conduct in his 18 months on the job at the Tucson computer center. (He added that at his previous post at San Francisco International Airport, forensic searches were done right at the airport.) Similarly, one of the border agents testified that this was the first case he was aware of in which electronic devices were turned over to Immigrations and Customs Enforcement for forensic examination, and that even cursory reviews of laptops for information about illegal drug trading occurred “no more than five” times during agent’s three-plus years at the Lukeville border station. See Michael Chertoff, Secretary of Homeland Security, *Searches Are Legal, Essential*, USA Today, July 16, 2008 (“Of the approximately 400 million travelers who entered the country last year, only a tiny percentage were referred to secondary baggage inspection for a more thorough examination. Of those, only a fraction had electronic devices that may have been checked.”).

States. See *Robinette*, 519 U.S. at 39 (“[W]e have consistently eschewed bright-line rules, instead emphasizing the fact-specific nature of the reasonableness inquiry.”); see also *Lyng v. Nw. Indian Cemetery Protective Ass’n*, 485 U.S. 439, 445 (1988) (“A fundamental and longstanding principle of judicial restraint requires that courts avoid reaching constitutional questions in advance of the necessity of deciding them.”).

Moreover, border agents are not free to undertake “unfettered crime-fighting searches or an unregulated assault on citizens’ private information.” Majority at 26. As I explained in my concurrence in *Seljan*, Congress and the Executive Branch have (and have exercised) the authority to restrict when and how border agents conduct searches. See *Seljan*, 547 F.3d at 1012 (Callahan, J., concurring) (citing, e.g., 19 U.S.C. § 1583; 19 C.F.R. § 145.3(b)-(c)); see also Yule Kim, Cong. Research Serv. RL34404, *Border Searches of Laptop Computers and Other Electronic Storage Devices*, 13–14 (2009) (describing recent legislative proposals to limit border searches of electronic devices). In a similar vein, Justice Breyer has noted that “Customs keeps track of the border searches its agents conduct, including the reasons for the searches. This administrative process should help minimize concerns that [border] searches might be undertaken in an abusive manner.” *Flores-Montano*, 541 U.S. at 156 (Breyer, J., concurring) (internal citation omitted).¹²

¹² See also U.S. Customs & Border Protection, Directive No. 3340-049, *Border Search of Electronic Devices Containing Information*, 3–9 (2009) (describing procedures for, and limits on, border searches of electronic devices).

Apart from being unnecessary, the majority's new limits on the government's border search authority will make it much harder for border agents to do their jobs, for at least two reasons. First, it is common knowledge that border agents at security checkpoints conduct more thorough searches not simply of those persons who arouse suspicion but also of a percentage of travelers on a random basis. Otherwise, a person who appears entirely innocent will have nothing to fear and will not be deterred from carrying something that should not be brought into the country. A checkpoint limited to searches that can be justified by articulable grounds for "reasonable suspicion" is bound to be less effective.

Second, courtesy of the majority's decision, criminals now know they can hide their child pornography or terrorist connections in the recesses of their electronic devices, while border agents, fearing Fourth Amendment or *Bivens* actions, will avoid conducting the searches that could find those illegal articles. The result will be that people and things we wish to keep out of our country will get in—a result hardly in keeping with our "inherent authority to protect, and a paramount interest in protecting," the "territorial integrity" of the United States. *Flores-Montano*, 541 U.S. at 153. The border search doctrine *must* account for the fact that border agents may need time and forensics to bypass "evasive actions" a criminal has taken to hide contraband or other illegal articles from plain view. *Montoya de Hernandez*, 473 U.S. at 542–43. I would rather leave those difficult decisions "to the discretion of the officers in the field who confront myriad circumstances we can only begin to imagine from the relative safety of our chambers." *United States v.*

Williams, 419 F.3d 1029, 1034 (9th Cir.), *cert. denied*, 546 U.S. 1081 (2005).¹³

IV.

The border search exception to the Fourth Amendment may be just that—an exception—but it is, and must be, a mighty one. The government’s right and duty to protect our nation’s territorial integrity demand that the government have clear authority to exclude—and thus to find—those people and things we have decided are offensive, threatening, or otherwise unwanted. Recognizing this, the Supreme Court has only once required reasonable suspicion for border searches in the 125 years it has been reviewing them. In the remaining cases, the Court has eschewed bright-line rules, balancing tests, and sliding intrusiveness scales, alluding to the possibility of, but never finding, a “particularly offensive”

¹³ The majority insists that reasonable suspicion is a “modest, workable standard” that is applied in domestic stops of automobiles “and other contexts,” and that still allows “agents to draw on their expertise and experience.” Majority at 26, 27 n.14. The majority is wrong for at least three reasons. First, in making this argument, the majority reveals that it does not appreciate the crucial differences between domestic and border searches, despite those differences being spelled out in a century of case law. Those differences range from the legitimate expectation of privacy that people have in their property to the constraints government officials face in searching it. Second, a reasonable suspicion standard injects unnecessary judicial review where previously it was absent. Third, just because border agents *could* apply the reasonable suspicion standard does not mean they are, or should be, *constitutionally compelled* to do so. See *Ickes*, 393 F.3d at 507; *cf. Seljan*, 547 F.3d at 1011 (Callahan, J. concurring) (explaining that requiring border agents to apply a First Amendment exception to border searches “would require them to engage in the sort of decision-making process that the Supreme Court wished to avoid in sanctioning expansive border searches”).

search. The fact that electronic devices can store large amounts of private information, or that the government can search them forensically, does not make a thorough search of such devices “particularly offensive.” Rather, the Supreme Court and this court have wisely avoided making the reasonableness of a search turn on the nature of the property being searched, for the many reasons discussed above. The result has been a clear, well-understood, efficient, and effective rule that border searches are *per se* reasonable.

Regrettably the majority, dispensing with these well-settled, sensible, and *binding* principles, lifts our anchor and charts a course for muddy waters. Now border agents, instead of knowing that they may search any and all property that crosses the border for illegal articles, must ponder whether their searches are sufficiently “comprehensive and intrusive,” Majority at 17, to require reasonable suspicion, and whether they have such suspicion. In most cases the answer is going to be as clear as, well, mud. We’re due for another course correction.

M. SMITH, Circuit Judge, dissenting, with whom CLIFTON and CALLAHAN, Circuit Judges, join with respect to Part I:

I respectfully dissent. Until today, federal courts have consistently upheld suspicionless searches of electronic storage devices at the border. *See United States v. Arnold*, 533 F.3d 1003, 1008 (9th Cir. 2008), *cert. denied*, 555 U.S. 1176 (2009) (“[R]easonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.”); *see also United States v. Ickes*, 393 F.3d 501, 507 (4th Cir. 2005) (no finding

of reasonable suspicion required to search personal computers and disks at border); *United States v. Linarez-Delgado*, 259 Fed. Appx. 506, 508 (3d Cir. 2007); *United States v. McAuley*, 563 F. Supp. 2d 672, 677–78 (W.D. Tex. 2008); *United States v. Buntz*, 617 F. Supp. 2d 359, 365 (E.D. Pa. 2008). Yet the majority ignores these cases, rewrites long standing Fourth Amendment jurisprudence, and, in narrowing *Arnold*, creates a circuit split.

While I share some of the majority’s concerns about the steady erosion of our personal privacy in this digital age, the majority’s decision to create a reasonable suspicion requirement for some property searches at the border so muddies current border search doctrine that border agents will be left to divine on an ad hoc basis whether a property search is sufficiently “comprehensive and intrusive” to require reasonable suspicion, or sufficiently “unintrusive” to come within the traditional border search exception. Requiring border patrol agents to determine that reasonable suspicion exists prior to performing a basic forensic examination of a laptop or other electronic devices discourages such searches, leaving our borders open to electronically savvy terrorists and criminals who may hereafter carry their equipment and data across our borders with little fear of detection. In fact, the majority opinion makes such a legal bouillabaisse out of the previously unambiguous border search doctrine, that I sincerely hope the Supreme Court will grant certiorari, and reverse the holding in this case regarding the level of suspicion necessary to search electronic devices at the border, for the sake of our national security, and the consistency of our national border search law.

The Supreme Court rejected our last attempt to narrow the border search exception, cautioning us not to create “complex

balancing tests” for border searches of property except in the rarest of cases, where the search is “so destructive as to require” reasonable suspicion. *United States v. Flores-Montano*, 541 U.S. 149, 152, 156 (2004) (rejecting our proposed reasonable suspicion requirement in *United States v. Molina-Tarazon*, 279 F.3d 709, 713–17 (9th Cir. 2002)). “Time and again” the Court has concluded that border searches are “reasonable simply by virtue of the fact that they occur at the border.” *Id.* at 152–53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)).

Despite the Court’s clear ruling on the issue, the majority again seeks to whittle away at the border search exception, this time by conjuring a reasonable suspicion requirement for border searches that employ computer software to search an electronic storage device. Why the use of computer software to analyze a hard drive triggers a reasonable suspicion requirement while a “manual review” of the same hard drive requires no suspicion, is left unexplained. Although technology may serve as a useful proxy for the intrusiveness of a search today, in the future even cursory searches might be more efficiently conducted by the use of such technology. Under the majority’s reasonable suspicion standard, individuals’ privacy rights are only as secure as the sophistication of the government’s current search mechanism.

Moreover, the task of distinguishing these “comprehensive and intrusive” laptop searches from the “unintrusive search” of a laptop affirmed in *Arnold*, 533 F.3d at 1008, or the search of a private letter affirmed in *United States v. Seljan*, 547 F.3d 993, 1003 (9th Cir. 2008) (en banc), leaves border patrol officers with a difficult choice: either protect our nation from those who mean us harm, or risk their own jobs and livelihood in a *Bivens* action, or disciplinary

proceedings. Apart from being administratively impractical, the majority's reasonable suspicion requirement disregards well established border search jurisprudence, and undermines vital national security interests. Ironically, the majority did not even need to consider the border search doctrine in this case because *the search at issue in this case did not occur at the border*.

Separately, but importantly, the majority's application of the reasonable suspicion requirement to Cotterman is also troubling. The majority purports to be concerned with travelers' "personal privacy and dignity," but its determination that reasonable suspicion exists under the exceedingly weak facts of this case undermines the liberties of U.S. citizens generally—not just at the border, and not just with regard to our digital data—but on every street corner, in every vehicle, and wherever else we rely on the doctrine of reasonable suspicion to safeguard our legitimate privacy interests.

I. The Border Search Doctrine

The majority heralds this as a "watershed" case that requires a narrowing of the border search exception to accommodate the privacy interests allegedly created by new technologies. Yet despite the majority's attempts to avoid the fact, the border search exception is clear and inflexible. The Supreme Court has repeatedly affirmed the breadth of the border search doctrine, extending a reasonable suspicion requirement only to: (1) "highly intrusive searches *of the person*"; (2) "searches of property [that] are so destructive as to require" reasonable suspicion; and (3) searches carried out in a "particularly offensive manner"—of which the Court has yet to find an example. *Flores-Montano*, 541 U.S. at 152,

154 n.2, 156 (quotations and citations omitted) (emphasis added).

The majority misconstrues these narrowly-defined exceptions, reading *Flores-Montano* to require reasonable suspicion whenever a search of property is deemed “overly intrusive.” Majority at 18–19. Yet, the exceptions articulated in *Flores-Montano* are far more circumscribed—applying not to “overly intrusive” searches of property, like the search of Cotterman’s computer, but only to “*highly* intrusive searches of the person.” *Flores-Montano*, 541 U.S. at 152 (emphasis added). The majority’s adoption of a reasonable suspicion requirement to “comprehensive forensic examination[s]” of property is irreconcilable with *Flores-Montano*. Majority at 6.

We have consistently rejected a reasonable suspicion requirement for border searches of expressive materials, such as papers and their modern-day equivalent—the data contained on electronic storage devices. *See, e.g., Seljan*, 547 F.3d at 1003 (“An envelope containing personal correspondence is not uniquely protected from search at the border.”); *Arnold*, 533 F.3d at 1008 (“[R]easonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.”). The majority states that its en banc decision narrows *Arnold* to permit only “relatively simple” border searches of laptops, and “not to countenance suspicionless forensic examinations.” Majority at 14 n.6. In narrowing *Arnold*, however, the court creates a circuit split regarding the application of reasonable suspicion to border searches of electronic devices. *See United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005); *see also United States v. Linarez-Delgado*, 259 Fed. Appx. 506, 508 (3d Cir. 2007).

For instance, in *Ickes* (as in *Arnold*) the defendant-appellant argued that a reasonable suspicion requirement was necessary for laptop searches at the border because otherwise “any person carrying a laptop computer [] on an international flight would be subject to a search of the files on the computer hard drive.” *Ickes*, 393 F.3d at 506–07. The Fourth Circuit rejected this argument, noting that

“[a]s a practical matter, computer searches are most likely to occur where—as here—the traveler’s conduct or the presence of other items in his possession suggest the need to search further. However, to state the probability that reasonable suspicions will give rise to more intrusive searches *is a far cry from enthroneing this notion as a matter of constitutional law*. The essence of border search doctrine is a reliance upon the trained observations and judgments of customs officials, *rather than upon constitutional requirements applied to the inapposite context of this sort of search*.”

Id. at 507 (emphasis added). The Third Circuit similarly rejected a reasonable suspicion requirement for border searches of electronic data, albeit in an unpublished opinion. *See United States v. Linarez-Delgado*, 259 Fed. Appx. 506, 508 (3d Cir. 2007) (“Data storage media and electronic equipment, such as films, computer devices, and videotapes, may be inspected and viewed during a reasonable border search.”) (citing *Ickes*, 393 F.3d 501). Because the majority has narrowed our holding in *Arnold* that “reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the

border,” *Arnold*, 533 F.3d at 1008, the Ninth Circuit stands alone, as it so often does.

The majority likens the search of Cotterman’s laptop to a “computer strip search,” Majority at 25, and proceeds to conflate the law regarding property searches with that regarding “highly intrusive searches of the person.” *Flores-Montano*, 541 U.S. at 152. However, 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 laptops, which know no dignity or shame, and thus have neither of those interests. *Flores-Montano*, 541 U.S. at 152 (emphasis added). Moreover, even genuine strip searches do not necessarily require reasonable suspicion at the border. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 541 n.4 (1985) (expressly declining to decide “what level of suspicion, *if any*, is required for . . . strip, body cavity, or involuntary x-ray searches”) (emphasis added).

The majority’s decision to insulate electronic storage devices from the border search exception unsettles the border search doctrine, places inappropriate burdens on law enforcement, reduces deterrence, and raises serious national security concerns. It also ignores the realities of electronic data transmission and the reduced privacy expectations that accompany much of this data, particularly at the border where “[t]he government’s interest in preventing the entry of unwanted persons and effects is at its zenith.” *Flores-Montano*, 541 U.S. at 152.

A. Burdens on Law Enforcement

The majority's holding cripples law enforcement at the border by depriving border patrol agents of the clear administrative guidance they need to carry out core law enforcement activities. "Officers who interact with those suspected of violating the law have an essential interest in readily administrable rules." *Florence v. Bd. of Chosen Freeholders of Cnty. of Burlington*, 132 S. Ct. 1510, 1522 (2012). Yet the majority's holding requires border patrol agents to determine on a case-by-case and moment-by-moment basis whether a search of digital data remains "unintrusive," *a la Arnold*, or has become "comprehensive and intrusive," *a la Cotterman*. Majority at 14, 17. Requiring law enforcement to make such complex legal determinations on the spot, and in the face of potentially grave national security threats, strips agents of their necessary discretion and deprives them of an efficient and administrable rule.

The majority dismisses the burden its reasonable suspicion requirement places on law enforcement, asserting that agents can simply "draw on their expertise and experience" to make the necessary judgment calls. Majority at 26. Yet rather than actually deferring to this expertise and experience, the majority forces border patrol agents to justify their decisions under a heightened standard that has never before been applied to border searches of property.

Border patrol agents process hundreds of thousands of travelers each day and conduct thousands of searches on

electronic devices each year.¹ Identifying national security and criminal threats at the border requires a high level of experience and discretion in order to recognize and respond to the ever-changing tactics of those who seek to enter our country with nefarious intent. In recognition of these crucial interests, the border search exception provides law enforcement with broad discretion to conduct border searches of property without resorting to case-by-case determinations of reasonable suspicion—determinations border patrol agents are ill-equipped to handle. *See generally Florence*, 132 S. Ct. at 1522 (rejecting reasonable suspicion requirement for prison strip-searches under this rationale). Moreover, as a practical matter, suspicionless border searches of property make sense, in light of the sheer number of individuals crossing the border with electronic devices each day. *See United States v. Martinez-Fuerte*, 428 U.S. 543, 557 (1976) (requiring reasonable suspicion for vehicle checkpoints near the Mexican border “would be impractical because the flow of traffic tends to be too heavy to allow the particularized study of a given car”). Given these realities of law enforcement at the border, a reasonable suspicion requirement for all “overly intrusive” electronic searches is simply not practicable.

B. National Security Concerns

The majority’s decision to insulate electronic devices from search at the border creates serious national security concerns. An “ever present threat exists from the potential for terrorists to employ the same smuggling and transportation networks, infrastructure, drop houses, and other support” as other illegal aliens. U.S. Customs and

¹ Department of Homeland Security Privacy Office, Annual Report to Congress 54 (2009).

Border Protection, National Border Patrol Strategy 5 (2005). The Department of Homeland Security has found that border searches of electronic storage devices are “essential” for “detect[ing] evidence relating to terrorism and other national security matters.”² Terrorists rely on electronic storage devices, for example, to copy and alter passports and other travel documents.³ By providing special privacy protections for electronic devices at the border, the majority eliminates the powerful deterrent of suspicionless searches and significantly aids technologically savvy terrorists and criminals who rely on encryption and other surreptitious forms of data storage in their efforts to do harm. *See Martinez-Fuerte*, 428 U.S. at 557 (rejecting reasonable suspicion requirement for vehicle checkpoints near the Mexican border because to hold otherwise “would largely eliminate any deterrent to the conduct of well-disguised smuggling operations”).

The majority contends that the goal of deterrence does not justify “any manner of intrusive search” at the border. Majority at 26. Although I certainly agree with the majority that a policy objective like deterrence cannot justify an otherwise unconstitutional “highly intrusive search[] of the person” at the border, *Flores-Montano*, 541 U.S. at 152, the crucial role of deterrence cannot, and should not, be understated. In fact, the Supreme Court recently affirmed the importance of deterrence in upholding suspicionless *strip*

² U.S. Customs and Border Protection, Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-049 § 1 (2009).

³ Thomas R. Eldridge, *et al.*, 9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States 60 (2004).

searches—the apotheosis of an intrusive search. *Florence*, 132 S. Ct. at 1516 (rejecting reasonable suspicion requirement for prison strip searches and reasoning that “detering the possession of contraband depends in part on the ability to conduct searches without predictable exceptions”). The suspicionless strip search upheld in *Florence*, which included a close visual inspection of “the buttocks or genital areas,” was unquestionably more intrusive than the so-called “computer strip search” at issue here. *Id.* at 1515.

The majority contends that the deterrence function of suspicionless searches will not be hampered by the requirement of reasonable suspicion because, “as a matter of commonsense and resources, it is only when reasonable suspicion is aroused that such searches typically take place.” Majority at 27 n.14. This is, of course, the very argument rejected by the Fourth Circuit in *Ickes*. See *Ickes*, 393 F.3d at 507 (“As a practical matter, computer searches are most likely to occur where—as here—the traveler’s conduct or the presence of other items in his possession suggest the need to search further. However, to state the probability that reasonable suspicions will give rise to more intrusive searches is a far cry from enthroning this notion as a matter of constitutional law.”).

In addition to undermining deterrence, a reasonable suspicion requirement will likely disincentivize agents to conduct laptop searches in close cases. See *Florence*, 132 S. Ct. at 1522 (“To avoid liability” if required to find reasonable suspicion, “officers might be inclined not to conduct a thorough search in any close case, thus creating unnecessary risk for the entire jail population.”). Border patrol agents accused of conducting an “unreasonable” search

face very real consequences—as federal officials, for example, they may be sued in their individual capacities for civil damages, as part of a *Bivens*⁴ action. See Ronald J. Sievert, *Meeting the Twenty-First Century Terrorist Threat Within the Scope of Twentieth Century Constitutional Law*, 37 Hous. L. Rev. 1421, 1424 (2000). The majority’s reasonable suspicion requirement saddles border patrol agents with a “Sophie’s choice” between securing our nation, and protecting their own livelihoods. These misaligned incentives create unnecessary risk, not just for a prison population, as in *Florence*, 132 S. Ct. at 1522, but for our entire nation.

C. Expectation of Privacy in Electronic Data at the Border

The majority suggests that travelers at the border have a heightened expectation of privacy in their electronic storage devices, due to the “uniquely sensitive nature of [this] data.” Majority at 25. There is no question that searches of electronic data are protected by the Fourth Amendment, but we have never found this data to be immune from the border search exception. In fact, these electronic storage devices are hardly a bastion of privacy. When connected to the Internet, they transmit a massive amount of intimate data to the public on an almost constant basis, rendering it unremarkable that they can be searched at the border, where “[t]he government’s interest in preventing the entry of unwanted persons and effects is at its zenith.” *Flores-Montano*, 541 U.S. at 152.

Indeed, Facebook, for example, now has more than 500 million users, who share more than 25 billion pieces of data

⁴ *Bivens v. Six Unknown Fed. Narcotics Agents*, 403 U.S. 388 (1971).

each month.⁵ Those who opt out of social networking sites are no less susceptible to the ubiquitous Internet cookie, which collects data on users' Internet activities to share or sell with other organizations. Max Stul Oppenheimer, *Consent Revisited*, 13 No. 12 J. Internet L. 3, 4 (2010). Until recently, a federally funded data accumulation system allowed clients to “search tens of billions of data records on individuals and businesses in mere seconds.”⁶ Considering the steady erosion of our privacy on the Internet, searches of electronic storage devices may be increasingly akin to a well-placed Internet search. Ironically, the majority creates a zone of privacy in electronic devices at the border that is potentially greater than that afforded the Google searches we perform in our own homes, and elsewhere.

The majority muses that “[a] person’s digital life ought not be hijacked simply by crossing the border,” Majority at 22, but it fails to explain why electronic data deserves special protections when we have never extended such protections to the same data in written form. *See Seljan*, 547 F.3d at 1003 (“An envelope containing personal correspondence is not uniquely protected from search at the border.”); *see also United States v. Tsai*, 282 F.3d 690, 696 (9th Cir. 2002) (no reasonable suspicion needed to search a traveler’s briefcase); *United States v. Grayson*, 597 F.2d 1225, 1228–29 (9th Cir. 1979) (no reasonable suspicion needed to search papers found

⁵ Jeffrey Rosen, *The Deciders: Facebook, Google, and the Future of Privacy and Free Speech*, in *Constitution 3.0: Freedom and Technological Change (Constitution 3.0)* 76 (Jeffrey Rosen & Benjamin Wittes eds., Brookings Institution Press 2011).

⁶ Christopher Slobogin, *Is the Fourth Amendment Relevant?*, in *Constitution 3.0* 18 (citing Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. Crim. L. & Criminology 1059, 1150–51 (2006)).

in a shirt pocket); *Henderson v. United States*, 390 F.2d 805, 808 (9th Cir. 1967) (no reasonable suspicion needed to search a traveler’s “purse, wallet, or pockets”). The documents carried on today’s smart phones and laptops are different only in form, but not in substance, from yesterday’s papers, carried in briefcases and wallets. The majority contends that electronic devices hold data of a “uniquely sensitive nature” and that, inexplicably, these devices have the “capability to . . . augment the expectation of privacy.” Majority at 23, 25. *Under the majority’s reasoning, the mere process of digitalizing our diaries and work documents somehow increases the “sensitive nature” of the data therein, providing travelers with a greater expectation of privacy in a diary that happens to be produced on an iPad rather than a legal pad.* Such artificial and arbitrary distinctions cannot serve as a reasonable basis for determining privacy rights at the border.

The majority attempts to distinguish electronic devices from papers by the vast amount of data they can hold, noting that “[a] car full of packed suitcases . . . cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage.” Majority at 21. Yet, “case law does not support a finding that a search which occurs in an otherwise ordinary manner, is ‘particularly offensive’ simply due to the storage capacity of the object being searched.” *Arnold*, 533 F.3d at 1010. The majority contends that it “discuss[es] the typical storage capacity of electronic devices simply to highlight the features that generally distinguish them from traditional baggage.” Majority at 21 n.10. Yet why the majority would bother to distinguish between the storage capacities of electronic devices and traditional luggage is a mystery, unless to support its enhanced protections for electronic devices based on their greater storage capacity.

Mapping our privacy rights by the amount of information we carry with us leads to unreasonable and absurd results. Under the majority's reasoning, a Mini Cooper filled with documents is entitled to less privacy protection at the border than a stretch Rolls-Royce filled with documents; a pickup truck filled with documents is entitled to less protection than an 18 wheeler filled with documents. It appears that those who cannot afford a 64 gigabyte iPad, or the "average" 400 gigabyte hard drive discussed by the majority, Majority at 20, will alone be subject to suspicionless searches. The majority's reasoning also protects the rich (who can generally afford more sophisticated devices) to a greater extent than the poor (who are presumably less able to afford those more capable devices.) See *United States v. Ross*, 456 U.S. 798, 822 (1982) ("[A] traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim[s] an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attache case.").

If our privacy interests are to be dictated by the quantity of data we possess, the question then becomes, how many gigabytes of storage must one buy to secure the guarantee that reasonable suspicion will be required before one's devices are searched? The majority gives us no firm basis for deciding how much storage space is necessary—32 gigabytes? 64 gigabytes? 400 gigabytes? Who knows? Moreover, the majority's test must constantly change to accommodate the ever-increasing capacity of electronic storage and new technologies. Before we know it, today's "average" 400 gigabyte hard drive will look like yesterday's diary next to tomorrow's "average" 2 terabyte hard drive.

The majority asserts that our "reasonableness determination must account for differences in property."

Majority at 24. This assertion has no basis in law, however, since *Flores-Montano* distinguished not between types of property, but between searches of property and “searches of the person.” *Flores-Montano*, 541 U.S. at 152 (emphasis added). In any event, it appears that the majority’s reasonableness requirement accounts not for “differences in property,” as it suggests, but rather for differences in the *intrusiveness* of a particular property search. As discussed *supra*, however, these intrusiveness-based tests have no place in border searches of property and have been explicitly rejected by the Supreme Court as “[c]omplex balancing tests.” *Flores-Montano*, 541 U.S. at 152.

The majority additionally speculates about the privacy implications of searching an external cloud platform, which may “includ[e] the same kind of highly sensitive data one would have in ‘papers’ at home.” Majority at 23. I share the majority’s keen interest in the Fourth Amendment implications of this burgeoning technology, but the reasonableness of cloud computing has no bearing on the case at hand, absent any facts that Cotterman utilized such a platform, or that such a platform was searched.

II. Waiver

There is another important issue in this case that is separate from the majority’s new standard for border searches. Specifically, I refer to the majority’s finding that there was reasonable suspicion to search Cotterman’s computer and other electronic devices, miles from the border. In its zeal to cripple the application of the current border search doctrine, while still securing Cotterman’s conviction, the majority turns on their heads all the parties’ arguments about reasonable suspicion as to Cotterman, and the findings

made by the lower courts concerning that suspicion. First, the majority now stakes its holding on a finding of reasonable suspicion—despite the fact that the government knowingly and unequivocally *conceded* on appeal any argument that the computer search was supported by reasonable suspicion. Second, the majority’s determination that reasonable suspicion was required under the border search exception is contrary to every argument raised by either party in its briefs *prior to* our request for supplemental briefing. Third, even the majority seems to concede that the search of Cotterman’s own computer that *actually occurred at the border* did not involve a computer with sufficient storage capacity, and was not sufficiently intrusive, to require reasonable suspicion, under its “new” border search doctrine. Thus, it need not have treated, nor altered, the current border search exception. Fourth, the Magistrate Judge’s Report and Recommendation, adopted by the District Judge, did not conclude that reasonable suspicion was required under the border search exception. Despite all the above, the majority upholds Cotterman’s conviction on grounds that the government had reasonable suspicion to extensively search his computer 170 miles from the border. Being mindful that the government has the burden of proof in this case, not the majority of our panel, I would have heeded the government’s strategic, good faith decision to abandon on appeal its argument that reasonable suspicion existed.⁷

The majority claims that Cotterman has not been prejudiced—despite the fact that the majority’s finding of reasonable suspicion is the *raison d’être* for his

⁷ When asked during oral argument why it failed to argue reasonable suspicion on appeal, the government acknowledged that the issue was a “close” one.

conviction—because Cotterman was allowed to file a supplemental brief on the matter after oral argument. Although I concede that what the majority did is technically permissible, *see U.S. Nat’l Bank of Oregon v Indep. Ins. Agents of Am., Inc.*, 508 U.S. 439, 446 (1993) (“When an issue or claim is properly before the court, the court is not limited to the particular legal theories advanced by the parties, but rather retains the independent power to identify and apply the proper construction of governing law”) (citations and quotations omitted), it is clear to me that *Cotterman has been severely prejudiced*, because his conviction is based solely on an issue the government conceded, and that Appellant, and the lower courts, took for granted because it was not needed for a border search. It is the majority of our panel, not the government, that prosecuted the reasonable suspicion issue in this case.

III. Extended Border Search

The extended border search doctrine applies to “searches that do not occur at the time of entry or in the immediate vicinity of the border.” *United States v. Alfonso*, 759 F.2d 728, 735 (9th Cir. 1985). Because these searches “intrude more on an individual’s normal expectation of privacy,” reasonable suspicion is required. *Id.* at 734.

The majority’s mutation of the border search exception is especially unnecessary given that *this search did not occur at the border*, but rather 170 miles away from the border and five days after the border was crossed. Indeed, the majority concedes that the government *could have* performed the forensic computer search at the border, but instead chose to transport Cotterman’s electronics more than 170 miles away. By labeling this a border search, the majority has conjured a

sort of “floating border,” whereby any item initially seized at the border, but not cleared there, can be transported thousands of miles away and searched anywhere, and at any time, simply because the government did not find anything (or enough) during its original search at the border. Because the search at issue occurred neither “at the time of entry or in the immediate vicinity of the border,” it is more appropriately analyzed as an extended border search. *See Alfonso*, 759 F.2d at 735.

The majority asserts that this case cannot be analyzed as an extended border search because Cotterman’s computer was never “cleared” at the border prior to search. Majority at 15. The majority is mistaken. In *United States v. Cardona*, 769 F.2d 625, 628 (9th Cir. 1985), we applied the extended border search doctrine to a search of a Federal Express package that occurred twenty-four hours *before* the scheduled border crossing, and 3,000 miles from the border. *See* 769 F.2d at 628 (“Considering the distance and time factors of the present case, we conclude that the facts of this case should be analyzed under the extended border search doctrine.”).

While this case presents issues we have not yet addressed in the context of an extended border search, *United States v. Alfonso* is squarely on point. In *Alfonso*, the government conducted an initial, cursory search of a ship upon its arrival at the Los Angeles harbor. *Alfonso*, 759 F.2d at 732. Thirty-six hours later, while still docked at the port, officials conducted a second, more intrusive search. *Id.* Tasked with determining whether the second search was an extended border search or a search at the functional equivalent of the border, we noted that “the instant case illustrates the difficulty of making sharp distinctions in this area.” *Id.* at

735. We determined that “[a]lthough we have no difficulty in relating this site with the border, we shall, because of the time factor—the lapse of thirty-six hours in conducting the searches—examine the facts under the rules of extended border search.” *Id.* at 734. The majority suggests that cases like *Alfonso* are distinguishable from the case at issue because those cases wrestled with distinguishing between a functional border search and an extended border search, whereas this case involves distinguishing between a traditional border search and an extended border search. This is a distinction without a difference since, as the majority acknowledges, there is no operative difference between border searches and searches that occur at the functional equivalent of the border, at least for purposes of determining whether a search is an extended border search.

I would hold that the search which took place 170 miles from the border, five days after crossing—a much greater lapse than the thirty-six hours in *Alfonso*—requires this case to be analyzed as an extended border search. Additionally, the reasonable suspicion requirement already applies to extended border searches, in recognition of the fact that such searches “intrude more on an individual’s normal expectation of privacy.” *Id.* As such, the extended border search doctrine is aptly suited to address the privacy expectations at issue in this case.

IV. Reasonable Suspicion

Irrespective of the government’s concession of the issue, the evidence in this case falls woefully short of reasonable suspicion. “[R]easonable suspicion exists when an officer is aware of specific, articulable facts which, when considered with objective and reasonable inferences, form a basis for

particularized suspicion.” *United States v. Montero-Camargo*, 208 F.3d 1122, 1129 (9th Cir. 2000) (en banc). We assess reasonable suspicion under the totality of the circumstances, “tak[ing] into account both factors weighing for and against reasonable suspicion.” *United States v. Manzo-Jurado*, 457 F.3d 928, 938 (9th Cir. 2006). We “will defer to officers’ inferences only when such inferences rationally explain how the objective circumstances ‘aroused a reasonable suspicion that *the particular person being stopped* had committed or was about to commit a crime.’” *Manzo-Jurado*, 457 F.3d at 934–35 (quoting *Montero-Camargo*, 208 F.3d at 1129) (alterations omitted). “Reasonable suspicion may not be based on broad profiles which cast suspicion on entire categories of people without any individualized suspicion of the particular person to be stopped.” *United States v. Sigmond-Ballesteros*, 285 F.3d 1117, 1121 (9th Cir. 2001) (internal quotations and citations omitted).

I agree with the majority that reasonable suspicion was not needed to conduct the initial search of Cotterman’s computer at the border, and that we analyze reasonable suspicion only as to the second search (the majority would say a continuation of the initial search,) which took place 170 miles from the border and several days after the border crossing. The majority’s reasonable suspicion finding appears to be based *solely* on the TECS alert: it states that “the nature of the alert on Cotterman, directing agents to review media and electronic equipment for child pornography, justified conducting the forensic examination despite the failure of the first search to yield any contraband.” Majority at 33. Thus, the majority pins reasonable suspicion on the TECS alert, dismisses out of hand the numerous factors weighing against reasonable suspicion, *and paves the*

way for a government database to target “entire categories of people without any individualized suspicion of the particular person to be stopped.” *Sigmond-Ballesteros*, 285 F.3d at 1121 (internal quotations and citations omitted) (emphasis added). The majority considers the TECS alert to be a sufficient basis for reasonable suspicion, but in reality, it is nothing more than a mechanism that automatically flags all individuals who are registered sex offenders in California—no matter the nature of the sex offense or how old the conviction—who travel frequently.⁸ California is home to more than 106,000 sex offenders.⁹ Some of these individuals are required to register as sex offenders for life. Depending on how many of them travel frequently, a TECS hit could affect tens of thousands of Californians—many with decades-old convictions. The TECS database clearly hits on “a very large category of presumably innocent travelers, who would be subject to virtually random seizures were the Court to conclude that as little foundation as there was in this case could justify a seizure.” *Reid v. Georgia*, 448 U.S. 438, 441 (1980). By allowing reasonable suspicion to rest entirely on the TECS alert, the majority rules that a decades-old conviction can serve as a basis to deprive a person of his or

⁸ The TECS alert is part of Operation Angel Watch, a program that targets California residents who are registered sex offenders based on the suspicion that those individuals who travel internationally are engaging in child sex tourism. The majority at one point improperly lists “the parameters of the Operation Angel Watch program” as an independent factor supporting reasonable suspicion. Majority at 30–31. We must look solely at the underlying *facts* supporting reasonable suspicion—*i.e.*, Cotterman’s status as a sex offender and his frequent travel—rather than the database or mechanisms used to deliver that information.

⁹ Press Release, National Center for Missing and Exploited Children, Number of Registered Sex Offenders in the US Nears Three-Quarters of a Million (Jan. 23, 2012).

her property for an indefinite period, so that a “border search” may be conducted hundreds of miles from the border.

The majority suggests that the TECS alert informed border patrol agents of the nature of Cotterman’s conviction. In fact, the TECS hit did not state the nature of Cotterman’s conviction, although one agent mistakenly recollected that “it stated that [Cotterman] appeared to [sic] been involved in some type of child pornography.” Curiously, another agent stated that a criminal history check on Cotterman revealed that “that he had a prior conviction pertaining to child pornography.” In fact, and despite the erroneous contentions of the referenced agents, Cotterman had no prior child pornography conviction; he had a 15-year-old conviction for sexual conduct with a minor. While we generally give “due weight to inferences drawn” by law enforcement, *Ornelas v. United States*, 517 U.S. 690, 699 (1996), the case for deference is questionable here in the absence of any rational explanation as to how the officers could have read the TECS alert and criminal history check, neither of which listed a conviction for child pornography, and come away thinking that Cotterman was guilty of that offense. *See Manzo-Jurado*, 457 F.3d at 934–35 (“[W]e will defer to officers’ inferences only when such inferences rationally explain how the objective circumstances aroused a reasonable suspicion.”); *see also Liberal v. Estrada*, 632 F.3d 1064, 1078 (9th Cir. 2011) (mistake of fact must be reasonable).

All things considered, the fact that an individual with a 15-year-old sex conviction was also a frequent traveler appears to be a rather weak lynchpin for reasonable suspicion. Yet, other than Cotterman’s prior conviction and travels, the factors cited by the majority are far too generalized to provide even an indicia of suspicion that Cotterman was involved in

sex tourism. For instance, the majority considers Cotterman's "collection of electronic equipment" to be a factor supporting reasonable suspicion. In today's world, the fact that Cotterman and his wife each carried a laptop and digital camera when traveling internationally, as well as one video camera between them,¹⁰ is no more evidence of "sex tourism" than of any other kind of tourism.

Similarly, the fact that Cotterman was returning from Mexico fails to support a finding of reasonable suspicion. Mexico is a popular travel destination for Californians, including those who travel to Mexico for its beaches, culture and weather, and not for its sex tourism. Travel to Mexico simply does not support reasonable suspicion without more specific evidence that Cotterman traveled to a particular establishment, city, or even region, associated with sex tourism. *See United States v. Irving*, 452 F.3d 110, 114, 124 (2d Cir. 2006) (finding reasonable suspicion based on knowledge that suspect, a convicted pedophile and the subject of criminal investigation, had visited an orphanage in Mexico and had luggage with children's books and drawings). According to the Department of Justice, American sex tourism is a problem not only in Mexico, but also in Southeast Asia, Central and South America, and, to a lesser extent, Eastern Europe.¹¹ Under the majority's application of reasonable suspicion, an individual who committed a sex offense 30 years ago cannot visit the Charles Bridge in Prague, the Cristo Redentor in Rio de Janeiro, or even the "lost city" of Machu Picchu, without arousing a "reasonable"

¹⁰ The video camera was apparently Mrs. Cotterman's.

¹¹ U.S. Department of Justice, *The National Strategy for Child Exploitation Prevention and Interdiction*, A Report to Congress 36 (2010).

suspicion of sex tourism. Someone who was convicted of tax evasion 15 years ago, or any other kind of conviction listed on a federal database, and particularly one that involved the use of a computer, should also probably avoid visiting Switzerland or Luxemburg under the majority's new standard. The bottom line is that thousands of individuals—many with decades-old convictions—will now be forced to reconsider traveling to entire countries or even *continents*, or will need to leave all their electronic equipment behind, to avoid arousing a “reasonable” suspicion.

Perhaps the most concerning aspect of the majority's opinion, especially given its stated stance on privacy rights at the border, is its readiness to strip former sex offenders and others convicted of past crimes (and who are, theoretically, entitled to be presumption of innocence) of even the most basic of privacy rights, such as the right to password-protect their electronic devices. The majority acknowledges that “it is commonplace for business travelers, casual computer users, students and others to password protect their files” and that “password protection is ubiquitous.” Majority at 31. It avers that “[n]ational standards *require* that users of mobile electronic devices password protect their files,” and that “[c]omputer users are routinely advised—and in some cases, required by employers—to protect their files when traveling overseas.” Majority at 31 (emphasis added). Yet because border patrol agents encountered a *single password-protected file* on Cotterman's computer, the majority considers password protection a factor contributing to reasonable suspicion.¹² Worse still, the majority contends that it is

¹² The unequivocal testimony of Agent Antonio Alvarado confirms that only a single password-protected file was discovered on Cotterman's computer at the border.

justified in considering the password-protected file because “making illegal files difficult to access makes perfect sense for a suspected holder of child pornography.” Majority at 32. I fail to see how the agents had reasonable suspicion that Cotterman’s computer contained “illegal files” based solely on his 15-year-old sex offense, travel to Mexico with his wife, and the “ubiquitous” act of password-protection. Indeed, as the majority acknowledges, making *legal* files difficult to access makes “perfect sense” for anyone, even former sex offenders.

I would find a password-protected file to be *not at all* suspicious, unless we want to start basing reasonable suspicion on locked diaries and briefcases. Registered sex offenders face numerous consequences as a result of their convictions, but the law has never before punished them for using “ubiquitous” and “commonplace” password-protection. Yet under the majority’s analysis, an individual traveling to Southeast Asia for business, who happens to be subject to one of TECS’s broad-based alerts, and who follows his company’s security protocols, should expect to have his electronic equipment seized and transported hundreds of miles away.¹³

Moreover, the majority fails to consider reasonable suspicion in light of the totality of the circumstances because

¹³ The majority finds ironic my concern about the expansiveness of its reasonable suspicion standard, since at the border, I would advocate for no suspicion at all. The majority is correct that at the border, my concern is simply with following *Flores-Montano* and maintaining national security. I view the majority’s application of its reasonable suspicion requirement as a separate issue, and my concern there is that the majority has so diluted the reasonable suspicion requirement as to undermine the rights of U.S. citizens generally.

it dismisses without explanation numerous factors that weigh *against* a finding of reasonable suspicion in this case. *See Manzo-Jurado*, 457 F.3d at 938 (the reasonable suspicion determination must “take[] into account both factors weighing for *and against* reasonable suspicion.”) (emphasis added). At the time the border patrol agents commenced the second search, 170 miles away from the border, any suspicions they may have initially harbored against Cotterman would have been largely addressed by their interrogations of Cotterman and his wife, which produced nothing suspicious. An initial search of Cotterman’s computer and the digital cameras turned up nothing more than a single password protected file and photos of “whale hunting and various excursions,” all of which corroborated Cotterman’s story about vacationing in Mexico. Also during this initial search, one of the border patrol agents did a records check and discovered that Cotterman’s conviction for the sex offense had occurred more than 15 years ago. Cotterman was fully cooperative and even offered to help the agents access his computer. The majority contends that Cotterman’s offer to help does not weigh against a finding of reasonable suspicion because the agents declined Cotterman’s offer based on the possibility—however slight—that Cotterman could “booby trap” the devices. That the agents were unable to accept Cotterman’s offer, however, does not change the reasonable inference that his offer was a genuine one.

Accordingly, it is irrelevant whether there was reasonable suspicion for the initial search, because I agree with the majority that reasonable suspicion was not required. The relevant inquiry here is what suspicion existed after all of Cotterman’s electronics were searched, and he and his wife were interrogated separately, and every piece of evidence

obtained corroborated the Cottermans' story about vacationing in Mexico. The only hint of suspicion remaining at that point—after the initial border search and interrogations—was the single password-protected file, which I agree with the majority is insufficient, by itself, to sustain a finding of reasonable suspicion. *See Manzo-Juardo*, 457 F.3d at 935 (“[T]o establish reasonable suspicion, an officer cannot rely solely on generalizations that, if accepted, would cast suspicion on large segments of the lawabiding population.”).

V. Conclusion

Reasonable suspicion has no place in property searches at the border, as the Supreme Court has consistently held. *See Flores-Montano*, 541 U.S. at 152–53 (“Time and time again, we have stated that searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.”). Imposing a reasonable suspicion requirement here forces courts and border patrol agents to engage in just the “sort of decision-making process that the Supreme Court wished to avoid in sanctioning expansive border searches.” *Seljan*, 547 F.3d at 1011 (citation omitted) (Callahan, J. concurring). Rather than rewrite the border search exception, as the majority does, I would affirm the district court’s application of the extended border search doctrine to Cotterman’s case, which appears most appropriate given the extensive lapse in distance and time between the first and the second search. Additionally, I would hold the government to its burden of proof in determining that reasonable suspicion was absent here. Under the doctrine of this case, the majority sweeps in thousands of innocent individuals whose electronic equipment can now be taken

82 UNITED STATES V. COTTERMAN

away from the border and searched indefinitely, under the border search exception.

I respectfully dissent.