SEARCHES WITHOUT BORDERS

CBP's Warrantless Searches of American Citizens on U.S. Soil

OCTOBER 23, 2019

STOP SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

STROOCK

INTRODUCTION

Virtually from its inception, the United States has sought to protect its citizens from unreasonable searches and seizures by the government. The Fourth Amendment expressly protects individuals' rights and privacy from potentially invasive and abusive searches of their "persons, houses, papers, and effects." However, there are certain exceptions to the protections afforded under the Fourth Amendment, the scopes of which have been expanded by the courts over the past 200 years as applied to a constantly evolving set of circumstances.

One such exception applies at our nation's borders. Traditionally, where individual rights clash with national interests, protections are weaker. Accordingly, under the "border search exception," when travelling into or out of the United States, searches of our persons and property are, under certain circumstances, permissible without a warrant in order to ensure that travelers have proper documentation, laws regulating the importation of goods are enforced, and the entry of harmful people or items is prevented.

Nevertheless, border searches still must balance the government's interests against an individual's privacy rights. This is becoming more difficult, however, in light of recent technological advancements resulting in increasingly sophisticated smartphones, tablets, and other electronic devices. As a result of these devices, people are "carrying" more and more information with them than ever before, including social security and credit card numbers, photos, emails, instant messages, contacts and internet search histories. Unchecked, the growing scope of the "border search exception" could undermine the Constitution's fundamental protections from warrantless, suspicionless searches.

Critically for travelers, the U.S. Customs and Border Protection ("CBP") has taken an expansive view of the border search exception which broadens its perceived authority to conduct warrantless searches, including of citizens' technology. In fact, citizens not even attempting to cross the border have been subjected to searches based solely on their mere proximity to the border.

In this paper, we present a case study involving a recent example of the CBP's attempt to expand its search authority at the border, provide an overview of the government's ability to conduct searches at our borders, and provide recommendations and "best practices" for carrying electronic devices at or across the border.

I. The CBP's Expansion of the Border Search Exception: A Case Study

In the summer of 2018, John Doe, a naturalized U.S. citizen of Arab descent arrived at the CBP's office at an international border crossing ("CBP Office"),[1] solely for the purpose of paying a duty on goods sent to him from outside the United States.

Generally, on prior visits to pay import duties, Mr. Doe would receive a call from customs at the airport (in the United States) at which the goods arrived, meet with the customs

[1] Due to privacy concerns, we have withheld John Doe's name and other personal information, as well as the location of the events described herein.

officer at the airport who inspected the goods and calculated the duty owed, and then follow the instructions provided to pay the duty at the CBP Office. Once at the CBP Office, Mr. Doe would speak with the supervisor, who would have received an email from the customs officer informing him of the duty owed and pay the amount. On no such prior visits did anyone at the CBP Office request Mr. Doe's identification or conduct a search.

Mr. Doe's attempt to pay an import duty in 2018 began as usual. He received a call from customs, drove to the airport, and met with the customs officer who inspected the goods. The customs officer provided Mr. Doe with a handwritten note expressly instructing him to go to the CBP Office and pay a small sum. After driving to CBP Office with two relatives, Mr. Doe entered the facility and approached a cashier, informing her that he was there to pay an import duty. When asked for identification, Mr. Doe explained that he did not have any with him (as he had forgotten his wallet at home), but that it was not necessary because he is a United States citizen and was not leaving the United States. He also asked the cashier to call the customs officer and check for an email regarding the duty owed.

It was at this point when CBP officers appeared and escorted Mr. Doe to a separate room for an inspection. The CBP officers requested his name, address, social security number and information about his citizenship. Mr. Doe, concerned and upset, again explained that he was only there to pay an import duty and mentioned that his relatives were waiting outside in the car. Rather than release Mr. Doe, the CBP officers instructed the two relatives to join Mr. Doe in the room. The CBP officers then instructed Mr. Doe to empty his pockets, which contained some cash, a pen, two cell phones, car keys and the handwritten instructions given to him by the customs officer. The CBP officers took Mr. Doe's keys and searched the vehicle without his consent, explaining that they were authorized to search it because he drove his car to the CBP Office.

Critically, the CBP officers also requested that Mr. Doe provide the passwords to unlock his cell phones. When he refused, the officers took the cell phones and placed them next to a computer. Though they did not appear to physically connect the cell phones to the computer or any device, the phones were out of Mr. Doe's vision for some time, and the CBP officers had physical control over the phones for a significant amount of time – long enough to copy encrypted digital data or other information using available forensic software.[2] After being detained for approximately one hour with his cell phones confiscated, Mr. Doe had his possessions returned and finally was allowed to pay his duty and leave.

Despite Mr. Doe repeatedly explaining that he was there only there to pay an import duty and showing written instructions from the customs officer at the airport, the CBP officers conducted an invasive, and arguably illegal, search of his cell phones and vehicle. Relying on an overly-expansive interpretation of the border search doctrine, the CBP officers apparently used Mr. Doe's mere presence at an international border as justification for the search.[3] Such invasive

[2] We are not aware of whether the CBP officers did, in fact, access and/or copy Mr. Doe's digital data or information.

[3] According to Mr. Doe, the CBP officers stated that, because he was at an international border, they had the right to do whatever they wanted.

and abusive conduct warrants an examination of the law relating to border searches, particularly with regard to our digital devices.

II. Warrantless Searches at the Border

a. *The Fourth Amendment's Border Search Exception*

The Fourth Amendment prohibits "unreasonable searches and seizures" by the government, and requires that law enforcement officials first obtain "probable cause" before a warrant may be issued.[4] A warrantless search is unreasonable under the Fourth Amendment unless one of a few "specifically established and well-delineated exceptions" applies.[5] Among these exceptions is the "border search exception," which 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."[6] Under this exception, government officials may conduct "routine" searches at the international border and its "functional equivalent"[7] without probable cause or suspicion of wrongdoing.[8] Nevertheless, though routine border searches are an exception to the warrant requirement, a border search must still be "reasonably related in scope to the circumstances which justified it initially."[9] In other words, there must be a balance of the government's interests with the individual's privacy interests. This balance is different at the border, where the state has "a paramount interest in protecting[] its territorial integrity," and an individual's "expectation of privacy is less at the border than it is in the interior."[10]

The contours of what qualifies as a "routine" border search as opposed to a "non-routine" border search have yet not been fully elucidated by the Supreme Court, though lower courts have expressed that "[t]he degree of invasiveness or intrusiveness associated with any particular type of search determines whether or not that search qualifies as routine."[11] Generally, routine border searches are those that do not pose a serious invasion of privacy or offend the average traveler.[12] Such searches can include pat-downs,[13] the removal of outer garments (*i.e.* jackets, hats, or shoes), the emptying of pockets, wallets, or purses,[14] and the inspection of luggage.[15]

---

[4] See U.S. CONST. amend IV.
[5] See Arizona v. Gant, 556 U.S. 332, 338 (2009).
[6] United States v. Ramsey, 431 U.S. 606, 620 (1977).
[7] See Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973) ("Whatever the permissible scope of intrusiveness of a routine border search might be, searches of this kind may in certain circumstances take place not only at the border itself, but at its functional equivalents as well."). Thus, the border's "functional equivalent" is usually the first practical detention point after a traveler crosses the border, and includes ports of entry or international airports. See id. at 272-73.
[8] See United States v. Montoya de Hernandez, 473 U.S. 531, 537-38 (1985).
[9] See id., 473 U.S. at 542.
[10] United States v. Flores-Montano, 541 U.S. 149, 153-54 (2004).
[11] United States v. Braks, 842 F.2d 509, 511-12 (1st Cir. 1988) (setting forth a non-exclusive factor test for determining the degree of invasiveness of a search); see also United States v. Vega-Barvo, 729 F.2d 1341 (11th Cir. 1984).
[12] See United States v. Johnson, 991 F.2d 1287, 1291 (7th Cir. 1993).
[13] See United States v. Beras, 183 F.3d 22, 24 (1st Cir. 1999).
[14] See United States v. Sandler, 644 F.2d 1163, 1169 (5th Cir. 1981).
[15] See United States v. Okafor, 285 F.3d 842 (9th Cir. 2002).

Non-routine border searches are those that involve a more serious invasion of an individual's privacy. The Supreme Court has suggested that "strip, body-cavity, or involuntary x-ray searches" would qualify as non-routine searches.[16] Destructive searches of property may also qualify as non-routine,[17] as may prolonged detentions.[18] Government officials must have "reasonable suspicion" of illegal activity before conducting a non-routine border search.[19] To establish reasonable suspicion, a law enforcement officer must have a "particularized and objective basis for suspecting the particular person" of wrongdoing.[20]

b. *How Border Search Law Applies to Electronic Devices*

In light of the increased prevalence of cell phones and tablets in everyday life, the border search doctrine is increasingly being applied to searches of electronic devices. Searches of electronic devices are often categorized as either manual, during which "officers review the contents of the device by interacting with it as an ordinary user would, through its keyboard, mouse or touchscreen interfaces," or forensic, during which officers "use sophisticated tools, such as software programs or specialized equipment, to evaluate information contained on a device, typically starting by making a copy of the device's data."[21] "Forensic searches can capture all active files, deleted files, files in allocated an unallocated storage space, metadata . . . password-protected or encrypted data, and log-in credentials and keys for cloud accounts."[22]

Initially, some courts treated non-forensic computer searches at the border as routine.[23] However, the border search doctrine, as applied to electronic devices, has been reshaped in the wake of the Supreme Court's decision in Riley v. California,[24] which held that the search-

[16] See Montoya de Hernandez, 473 U.S. at 541 n.4.
[17] See Flores-Montano, 541 U.S. at 155-56.
[18] See Montoya de Hernandez, 473 U.S. at 535 (finding a 16-hour detention of an alimentary canal smuggler to be non-routine, but supported by reasonable suspicion); see also United States v. Adekunle, 2 F.3d 559, 562 (5th Cir. 1993) (holding that the government "must seek a judicial determination, within a reasonable period, that reasonable suspicion exists to support" an extended detention).
[19] See Montoya de Hernandez, 473 U.S. at 541.
[20] Id. (citations omitted).
[21] See Alasaad v. Nielsen, No. 17-cv-11730, 2018 WL 2170323, at *2 (D. Mass. May 9, 2018) (internal quotations and citations omitted).
[22] Id. (internal quotations and citations omitted).
[23] See, e.g., United States v. Stewart, 729 F.3d 517, 525-26 (6th Cir. 2013) (concluding that the non-forensic examination of a laptop computer occurring twenty miles away from the international airport was a continuation of a routine border search and did not require reasonable suspicion); United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008) (holding that the Fourth Amendment does not protect electronic devices, including computers and cell phones, from warrantless and suspicionless searches in border context); United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007) (no reasonable suspicion required for a routine border search of "[d]ata storage media and electronic equipment, such as films, computer devices, and videotapes"); United States v. Ickes, 393 F.3d 501, 504 (4th Cir. 2005) (no suspicion required for computer search at the border); Abidor v. Napolitano, 990 F. Supp. 2d 260, 277–78 (E.D.N.Y. 2013) (dismissing the lawsuit for lack of standing, but nevertheless concluding that reasonable suspicion was not required for a laptop search); United States v. Bunty, 617 F. Supp. 2d 359, 365 (E.D. Pa. 2008) (no reasonable suspicion required to search through computer disks). By contrast, some courts began treating forensic computer searches as non-routine and requiring reasonable suspicion. See, e.g., United States v. Cotterman, 709 F.3d 952, 962 (9th Cir. 2013) (holding that "the comprehensive and intrusive nature of a forensic examination . . . trigger[s] the requirement of reasonable suspicion"); United States v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014).
[24] 573 U.S. 373 (2014).

incident-to-arrest exception does not extend to cell phones and that the Fourth Amendment requires police to obtain a warrant supported by probable cause to search a phone seized during arrest. The Court reasoned that the balancing of interests for searches of phones seized during arrest did not support extending the exception "to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[25] It continued that cell phones "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[26]

Although Riley did not involve the border search exception, circuit courts are now split on Riley's application in the border search context. Most courts continue to hold that manual searches of electronic devices are routine, while forensic searches are non-routine and require at least reasonable suspicion.[27] For example, courts in the Ninth Circuit have found that only manual searches of electronic devices are routine, and permissible without a warrant.[28] However, the Eleventh Circuit in United States v. Touset explicitly rejected Riley's application in the border search context and refused to hold that reasonable suspicion is required even for non-routine forensic searches of electronic devices.[29] The circuit split on this issue may result in the Supreme Court addressing the issue of whether Riley applies in the border search context.

Perhaps the most exhaustive treatment of Riley in the border search context is now being litigated in Alasaad, where the goal is to establish a precedent that Riley requires at least reasonable suspicion for manual border searches of electronic devices.[30] In Alasaad, eleven plaintiffs (ten U.S. citizens and one lawful permanent resident) alleged that ICE and CBP agents improperly searched their laptops and phones at the border in violation of the Fourth Amendment. The court, in denying defendants' motion to dismiss, held, in relevant part, that in the "absence of controlling precedent to the contrary, this Court cannot rule that [the Fourth Amendment principle espoused in Riley] would not extend in some capacity to the border."[31] In denying the motion to dismiss, the court appears to have left open the possibility that the warrant

[25] Id. at 385.
[26] Id. at 393.
[27] See, e.g., United States v. Mendez, 240 F. Supp. 3d 1005 (D. Ariz. 2017) (reading Riley to support that a warrant was not required for a manual search of the defendant's cell phone at the border); United States v. Cano, 222 F. Supp. 3d 876, 879 (S.D. Cal. 2016) (holding that although Riley "did not specifically address the border search exception, Riley does not preclude the application of such doctrine" in the border search context); United States v. Kolsuz, 185 F. Supp. 3d 843 (E.D. Va. 2016) (determining that a manual search of the defendant's iPhone was a routine border search while the subsequent forensic search was non-routine), aff'd United States v. Kolsuz 890 F.3d 133 (4th Cir. 2018); United States v. Kim, 103 F. Supp. 3d 32 (D.D.C. 2015) (applying the Riley balancing test and finding that evidence obtained from a forensic search of the defendant's laptop should be suppressed because the search was not supported by reasonable suspicion).
[28] See, e.g., United States v. Caballero, 178 F. Supp. 3d 1008, 1016, 1018, 1020 (S.D. Ca. 2016).
[29] 890 F.3d 1227, 1229 (11th Cir. 2018) ("[O]ur precedents about border searches of property make clear that no suspicion is necessary to search electronic devices at the border."). See also United States v. Feiten, No. 15-20631, 2016 WL 894452 (E.D. Mich. Mar. 3, 2016) (denying the defendant's motion to suppress evidence obtained from a forensic search of his laptop on the basis that such a search is a routine border search and Riley does not compel a different conclusion).
[30] 2018 WL 2170323.
[31] Id. at *20.

requirement under Riley may extend to border searches, though it is unclear whether that requirement would apply to routine searches, non-routine searches, or both.

In light of the Supreme Court's recent focus on the right to privacy in the digital age,[32] and given the privacy interests in today's electronic devices as articulated in Riley, the border search exception may someday evolve such that a CBP officer must have reasonable suspicion for even routine searches of electronic devices. However, as evidenced by its treatment of Mr. Doe, this is not the view the CBP takes.

c. *CBP's Current Policy Regarding Border Searches of Electronic Devices*

Despite the invasiveness and potential for Fourth Amendment violations, the CBP's current search policies still allow border officers, under certain circumstances, to manually search a U.S. citizen's phone or other electronic device with no warrant, level of suspicion, or probable cause whatsoever. CBP Directive number 3340-049A, issued January 4, 2018 (the "Search Policy"), governs border searches of electronic devices.[33] The Search Policy defines an "electronic device" as "[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players."[34] Consistent with case law, it divides electronic device searches into two categories: advanced searches and basic searches. An "advanced search" is "any search in which an Officer connects external equipment . . . to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents."[35] Advanced searches require "reasonable suspicion of activity in violation of the laws enforced or administered by CBP" or a "national security concern," and a supervisor must be present during such searches.[36] By contrast, a "basic search" is "[a]ny border search of an electronic devise that is not an advanced search."[37] Critically, under the Search Policy, basic searches may be conducted "with or without suspicion."[38]

The Search Policy requires that all electronic device searches be documented,[39] and that the searches "be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, officer safety, or other operational considerations that make it inappropriate to permit the individual to remain present."[40]

---

[32] See, e.g., Carpenter v. United States, ___ U.S. ___, 138 S. Ct. 2206, 2217 (2018) ("Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in Jones or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.").

[33] The Search Policy superseded Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008), to the extent they pertain to electronic devices, as well as CBP Directive No. 3340-049, Border Searches of Electronic Devices Containing Information (August 20, 2009).

[34] See Search Policy, § 3.2.

[35] Id. at § 5.1.4

[36] Id.

[37] Id. at § 5.1.3.

[38] Id.

[39] See id. at § 5.1.5.

[40] Id. at § 5.1.6.

Nevertheless, allowing an individual to remain present during a search does not entitle that individual to "observe the search itself."[41]

The Search Policy authorizes examination of only information that is "resident upon the device" as opposed to information stored remotely.[42] Thus, travelers may be required to provide "[p]asscodes and other means of access . . . to facilitate inspection of devices,"[43] because if an officer cannot complete an inspection because of password or other encryption, the CBP officer may "detain the device pending a determination as to its admissibility, exclusion, or other disposition,"[44] or "seek technical assistance" or "use external equipment" to access the device.[45]

d. *An Actual Border Crossing Is Generally Required For The Exception To Apply*

The experience of Mr. Doe, who was not even crossing an international border, begs the question of when, and under what circumstances, the border search exception authorizes CBP officers to conduct warrantless searches of our digital devices. As evidenced by the CBP's polices and the regulations on which they are based, the primary purpose of border searches is to allow the government to invoke its "longstanding right … to protect itself by stopping and examining persons and property crossing into this country."[46] Accordingly, courts addressing the border search exception generally have held that its application must be premised on the fact that the person or object searched has, in fact, crossed the international border. In Ramsey, a case involving the warrantless search of letters delivered from Thailand, the Supreme Court held that border searches "have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside" without the additional requirement that probable cause exist.[47] Thus, a demonstration "that the person or item in question had entered into our country from outside" should be required for the border search exception to apply.[48]

As the Fifth Circuit has stated, a "legion of cases have made clear that the propriety of a border search rests on the 'critical fact' of whether or not a border crossing has occurred."[49]

---

[41] Id.
[42] See id. at § 5.1.2.
[43] Id. at § 5.3.2.
[44] Id. at § 5.3.3.
[45] Id. at § 5.3.4.
[46] Flores-Montano, 541 U.S. at 152.
[47] 431 U.S. at 619.
[48] Id. at 620. ("The critical fact is that the envelopes cross the border and enter this country. … It is their entry from without it that makes a resulting search 'reasonable.'").
[49] United States v. Stone, 659 F.2d 569, 573 (5th Cir. 1981). See United States v. Victoria-Peguero, 920 F.2d 77, 80 (1st Cir. 1990) ("It is equally well established that border searches constitute such an exception and are reasonable 'by the single fact that the person or item in question had entered into our country from outside.'"); United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006) ("Although routine border searches of a person's belongings are made reasonable by that person's decision to enter this country, …."); United States v. Glasser, 750 F.2d 1197, 1201 (3d Cir. 1984) ("On a constitutional level, then, it is beyond question that agents of the federal government may, without cause, search persons and packages entering the country without violating the rights guaranteed by the Fourth Amendment."); United States v. Oriakhi, 57 F.3d 1290, 1297 (4th Cir. 1995) ("[W]e join the several other circuit courts which have held that the *Ramsey* border search exception extends to all routine searches at the nation's borders, irrespective of whether persons or effects are entering or exiting from the country."); United States v. Jackson, 825 F.2d 853, 858-59 (5th Cir. 1987) ("It is the *single fact* that the individual or item has entered this nation

Courts also have held that other concepts of the border search exception require an actual border crossing, including "functional equivalent of the border" searches, which are permitted without a warrant, suspicion, or probable cause just as if the search occurred at the international border line.[50] Similarly, under the "extended border search" doctrine, non-routine searches that occur "near the border" are "deemed constitutionally permissible if reasonable under the Fourth Amendment" where "(1) there is a reasonable certainty that a border crossing has occurred; (2) there is a reasonable certainty that no change in condition of the [item searched] has occurred since the border crossing; and (3) there is a reasonable suspicion that criminal activity has occurred."[51] Accordingly, under any border search doctrine on which the CBP could rely to conduct a warrantless search, it is likely that at least "the fact that a border crossing occurred must be demonstrated."[52]

On the other hand, the Sixth Circuit has held that certain searches at the border without a warrant, probable cause, or reasonable suspicion are permissible *even where there was no border crossing*. In United States v. Humphries, a motorist inadvertently stopped near the Detroit-Windsor Tunnel leading to Canada, where custom agents conducting warrantless searches of outbound vehicles discovered a small amount of marijuana and a gun.[53] Despite not having crossed the border, the Sixth Circuit affirmed the denial of the motorist's motion to suppress the evidence because, by being "within the area where cars normally lined up to undergo inspection

---

from outside that justifies the search. … Therefore, only searches of persons or effects that have crossed the border may be deemed functionally equivalent to border searches and hence be excepted from the Fourth Amendment's compass.") (citations omitted); United States v. Cortez-Rocha, 394 F.3d 1115, 1119 (9th Cir. 2004) ("In order to protect the country from the entry of drugs, weapons, explosives, and unauthorized persons and things, the government must be empowered to conduct searches of containers crossing an international border.") (internal citations omitted); United States v. Maigar, 568 F. Supp. 2d 245, 247 (N.D.N.Y. 2008) ("It has long been recognized that border searches are made reasonable by the person's decision to cross the border and thus are not violative of the Fourth Amendment's prohibition against unreasonable searches.").

[50] For example, in United States v. Graham, which involved a defendant who travelled on a ferry that originated in Canada, but who had both boarded and departed the ferry within the United States without crossing an international border, the court noted that "'only searches of persons or effects that have crossed the border may be deemed functionally equivalent to border searches and hence be excepted from the Fourth Amendment's compass.'" 117 F. Supp. 2d 1015, 1018 (W.D. Wash. 2000) (quoting Jackson, 825 F.2d at 859). Likewise, in United States v. Amuny, the Fifth Circuit held that the warrantless search of an airplane could not be sustained based on the "functional equivalent of border doctrine" because there was no reasonable certainty that the airplane had, in fact, crossed the border. 767 F.2d 1113, 1123 (5th Cir. 1985) ("To justify a search at the functional equivalent of the border, agents must demonstrate to a 'reasonable certainty' that the vehicle has, in fact, crossed the international border.") (citing cases).

[51] United States v. Yang, 286 F.3d 940, 945 (7th Cir. 2002); see also U.S v. Delgado, 810 F.2d 480, 483 (5th Cir. 1987).

[52] United States v. Delgado, 810 F.2d at 483, fn. 2 ("Our subsequent cases like Niver have made it clear, however, that an actual border crossing must be demonstrated to justify either a 'functional equivalent of the border' search or an 'extended border search.'"); see also United States v. Niver, 689 F.2d 520, 526 (5th Cir. 1982) ("The defendants contend, and we think rightly so, that whatever the type of search is involved, a border crossing must be demonstrated by more than reasonable suspicion or probable cause. We have generally required a showing beyond a 'reasonable certainty' that the entity searched has crossed the international border or a high degree of probability that a border crossing took place.") (internal citations and quotations omitted).

[53] 308 F. App'x. 892 (6th Cir. 2009).

before proceeding to Canada," the motorist was "close enough to the border, or its functional equivalent, to fall within the border search exception."[54]

Likewise, in D.E. v. Doe, the Sixth Circuit affirmed the dismissal of a plaintiff's Bivens federal civil rights action, holding that the CBP officers' unwarranted search of his motor vehicle was lawful under the border-search exception to the Fourth Amendment's probable cause requirements.[55] There, the plaintiff missed a turn while driving and inadvertently ended up at the international border crossing to Canada at the Blue Water Bridge in Michigan. Despite the fact that the plaintiff wished to turn around and *not* cross the border into Canada, the district court dismissed the action.[56] The Sixth Circuit affirmed, holding that "[b]ecause a traveler's subjective intent not to leave the country does not provide an exception to the government's authority to conduct suspicionless searches of vehicles at the border."[57]

A line of older cases also holds that certain persons who have direct contact with a border area, or whose actions are reasonably related to a border area, are subject to warrantless searches, even if there has been no border crossing, but only if an officer has reasonable suspicion of criminal activity.[58]

Accordingly, as explained above, except under certain limited circumstances involving a reasonable suspicion of criminal activity, and a few minority decisions in the Sixth Circuit, an actual border crossing should be required for the "border search exception" to justify a warrantless search of a person or property at the border. Under this standard, because Mr. Doe did not—and never intended to—cross the border into Canada, the search of Mr. Doe's cell phones (and vehicle) was invasive, abusive, and illegal.

III. Recommendations

In light of the CBP's expanding view of its perceived authority to conduct warrantless searches at our borders, all travelers should be aware of the individual risks relating to their

---

[54] Id. at 896.
[55] 834 F.3d 723 (6th Cir. 2016).
[56] See Ericksen v. Doe, No. 15-CV-10088 (GCS), 2015 WL 4041316, *3 (E.D. Mich. July 1, 2015) ("Given his location at the international border, customs agents could permissibly search his vehicle without probably cause, a warrant, or reasonable suspicion."). In dismissing the complaint, the district court relied, in part, on the "controlling Sixth Circuit precedent" under United States v. Humphries. Id.
[57] D.E., 834 F.3d at 725-27 ("That D.E. did not cross the border is irrelevant, as officers may conduct suspicionless searches on outbound persons and effects, which have not yet crossed the border, see United States v. Boumelhem, 339 F.3d 414, 420–23 (6th Cir. 2003). That D.E. subjectively did not intend to cross the border is also irrelevant. There is no reliable way for the CBP officers to tell the difference between a motorist who has just crossed the border or who intends to cross the border and a "turnaround motorist" who is at the border area by mistake.").
[58] United States v. Glaziou, 402 F.2d 8, 13-14 (2d Cir. 1968) ("Therefore, we hold that when an individual has direct contact with a border area, or an individual's movements are reasonably related to the border area, that individual is a member of the class of persons that a customs officer may, if his suspicions are aroused, stop and search while the individual is still within the border area.") (internal citations omitted). Similarly, in United States v. Hill, the Fifth Circuit upheld the warrantless search of a truck that had been loaded with boxes from a vessel, despite the fact there was no evidence that the vessel had crossed an international border. 430 F.2d 129, 131 (5th Cir. 1970) (holding that the "appellants were within the class of individuals subject to a 'border search', that the customs agents had a reasonable suspicion that they were in possession of unlawfully imported merchandise, and that the search was conducted within a border area.")

digital devices and make smart choices when travelling not just across the border, but near it. With that in mind, we offer a brief overview of some recent advances in forensic technology, which may allow CBP officers to search and collect a traveler's digital data even without a passcode. We also provide several "best practices" for travelling with digital devices at or near the border.

a. *Advances in Forensic Technology*

CBP and other law enforcement agencies increasingly turn to private sector firms for the tools necessary to forensically compromise and examine encrypted devices.[59] CBP frequently partners with Cellebrite, a firm that boasts the ability to decrypt the vast majority of phones and computers, including nearly every iPhone.[60] Cellebrite can "recover downloaded emails, third party application data, geolocation data and system logs."[61] The firm's Universal Forensic Extraction Device ("UFED") tool can even capture deleted text messages and call histories from certain devices and applications.[62] CBP's forensic searches have only increased in recent years, as the agency deployed more Cellebrite devices in more ports of entry.[63]

CBP and other law enforcement agencies have also spent millions of dollars contracting with GrayShift, a much newer company.[64] Its GrayKey decryption tool appears able to access certain newer iPhone models that are impervious to Cellebrite's analysis.[65] GrayKey also allows users to recover iPhone passwords, including third-party passwords saved on the phone's storage system.[66] Notably, GrayKey can harvest an iPhone's entire file system, providing users with deleted text messages, emails, and even Google searches from the iPhone and synced laptops and tablets.[67] Grayshift frequently updates GrayKey and other products to circumvent new and

[59] See Thomas Brewster, US Immigration Splurged $2.2 Million On Phone Hacking Tech Just After Trump's Travel Ban, FORBES, Apr 13, 2017, https://www.forbes.com/sites/thomasbrewster/2017/04/13/post-trump-order-us-immigration-goes-on-mobile-hacking-spending-spree/#7b2f58aba1fc.
[60] See Sean Gallaghar, Cellebrite Can Unlock Any iPhone (For Some Values Of "Any"), ARS TECHNICA, Feb 28, 2018, https://arstechnica.com/information-technology/2018/02/cellebrite-can-unlock-any-iphone-for-some-values-of-any/.
[61] See Thomas Brewster, The Feds Can Now (Probably) Unlock Every iPhone Model In Existence, FORBES, Feb 26, 2018, https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#661f52dc667a.
[62] See Kim Zetter, When The FBI Has A Phone It Can't Crack, It Calls These Israeli Hackers, THE INTERCEPT, Oct 31, 2016, https://theintercept.com/2016/10/31/fbis-go-hackers/.
[63] See id.
[64] See Thomas Brewster, Immigration Cops Just Spent A Record $1 Million On The World's Most Advanced iPhone Hacking Tech, FORBES, May 8, 2019, https://www.forbes.com/sites/thomasbrewster/2019/05/08/immigration-just-spent-a-record-1-million-on-the-worlds-most-advanced-iphone-hacking-tech/#5b7274a35a0a.
[65] See id.
[66] See id.
[67] See Thomas Brewster, Did Apple Just End The 'Golden Age' Of Government iPhone Hacking?, FORBES, Sept 21, 2018, https://www.forbes.com/sites/thomasbrewster/2018/09/21/can-apple-bring-an-end-to-the-golden-age-of-government-iphone-hacking/#320d848674eb.

improved security features from Apple and other manufacturers.[68] Advances in devices' security are sometimes overcome in a matter of weeks, or even days.

While Cellebrite, Grayshift, and other firms provide tools to access encrypted devices, they come at a steep cost. The expense of decrypting a single device on GrayKey, for example, can run into the tens of thousands of dollars.[69] This expense forces agencies to deploy some of the most powerful decryption tools selectively, leaving many phones and laptops unbroken.[70] So long as the time and expense of decrypting a device remains non-trivial, there will continue to be a significant benefit for users who protect their data with encryption and other techniques.

b. *Best Practices for Travelling at the Border*

Several low-cost or free steps can help protect electronic devices. Many phone users "lock" their devices with 4 or 6-digit numerical combination, but a longer passwords using a mix of letters, numbers, and symbols can exponentially increase the time needed to decrypt a device.[71] It is also important to use truly randomized password combinations and to avoid repeating passwords on multiples services or devices.[72]

Users may gain additional privacy protections by disabling biometric access features, such as fingerprint sensors of facial recognition. The Fifth Amendment, which can protect Americans from being forced to divulge our alphanumeric passwords, may not protect individuals from being forced to biometrically unlock their device.[73] You cannot be compelled to produce a testimonial communication, like a password, but some jurisdictions have held that you can be compelled to give your biometric data.[74]

Power off your devices. When turned off, your devices may be less vulnerable to wireless attempts to access your digital information. Keeping your devices off also often forces higher levels of security upon turning the device on, for example by forcing a passcode entrance upon turn-on rather than just a facial scan if that is your selected general security feature.

Where an individual refuses to unlock a device, CBP may detain it and attempt to break the device encryption and download all its data.[75] Many smartphones and laptops encrypt internal data by default, but not all use strong encryption, and some may leave external data, SD

[68] See Robert McMillan, Meet Apple's Security Headache: The GrayKey, a Startup's iPhone-Hacking Box, WALL ST. J., June 14, 2018, https://www.wsj.com/articles/the-hacking-box-that-led-to-a-golden-age-of-iphone-investigations-1528996893.
[69] See Don Reisinger, A Former Apple Security Engineer's Company Will Unlock Your iPhone X—for $15,000, FORTUNE, March 6, 2018, http://fortune.com/2018/03/06/apple-unlock-iphone/.
[70] See id.
[71] See David Nield, *What's the Most Secure Way to Lock Your Smartphone?*, GIZMODO, July 26, 2017, https://gizmodo.com/whats-the-most-secure-way-to-lock-your-smartphone-1796948710 (noting that experts prefer longer pins and randomly generated passwords that are harder to remember).
[72] *Id.*
[73] See State v. Diamond, 905 N.W.2d 870 (Minn.), cert. denied, 138 S. Ct. 2003 (2018) (holding that biometric information used to unlock a cellphone was not a testimonial communication but a password would be).
[74] See United States v. Wade, 388 U.S. 218, 222 (1967).
[75] See Mark Bergen, *What if San Bernardino Suspect Had Used an Android Instead of an iPhone?*, VOX, Feb. 21, 2016, https://www.vox.com/2016/2/21/11588052/what-if-san-bernardino-suspect-had-used-an-android-instead-of-an (discussing the vulnerability of unencrypted devices).

memory cards, completely unprotected.[76] If possible, choose the device settings that use the strongest form of encryption for your device's operating system. However, while strong encryption can extend the time needed to break into a device, it rarely can prevent access altogether.

Generally, the strongest protection against a border search is to avoid carrying a device at the time you transit. To the extent possible, leave your electronic devices behind. The less one carries with them, the less there is to search. This can be difficult for those that carry various types of technology for personal or professional use, including, but not limited to, laptop computers for work, a tablet for entertainment, a smartwatch for notifications, and of course one or several cell phones. However, it may be helpful to consider whether one such device can suffice on any particular trip. For example, if you have multiple cell phones for multiple uses, think about whether one or more can be left at home.

These best practices come with a caveat created by the Court's broad interpretation of 18 U.S.C. § 1519:[77] Deleting data or any conduct taken "intended to impede any federal investigation or proceeding" is a felony even if the investigation or proceeding is not "on the verge of commencement."[78] Therefore, any action taken to complicate an anticipated search of an electronic device by CBP opens you up to destruction of evidence and obstruction of justice charges.

[76] See Jason Cipriani, *What You Need to Know About Encryption on Your Phone*, CNET, Mar. 10, 2016, https://www.cnet.com/news/iphone-android-encryption-fbi/ (discussing the move by Apple and Android to automatically encrypt device data in 2014).
[77] See Yates v. U.S., 135 S. Ct. 1074, 1087 (2015).
[78] *Id.*

Surveillance Technology Oversight Project, Inc.

40 Rector Street
9th Floor
New York, NY, 10006

www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

STROOCK