Extraction, Retention, and Use: Applying Use-Restrictions to Fourth Amendment Forensic Electronic Device Search Doctrine at the Border

Daniel Vicente Alayo-Matos[†]

ABSTRACT

Forensic electronic device searches are a formidable weapon in a border protection agents' arsenal. Agents download the data from an electronic device and may store it for up to fifteen years, where it can be accessed by thousands Department of Homeland Security (DHS) agents with minimal controls. Annually, agents collect the forensic digital data of over 40,000 international travelers. The border constitutes an exception to typical Fourth Amendment protections against unreasonable searches and seizures, as officials may search individuals crossing the border without a warrant or reasonable suspicion. At least one circuit has held that the Fourth Amendment's protections pose no limit on whose or what electronic data may be collected when a traveler crosses the international border.

It is unacceptable to use the Fourth Amendment border exception to not only search, but also copy, retain, query, and share traveler data, with little evidence to support the action. Use of data gathered under the border exception should be limited to the purpose of the border exception: protecting the border. This Comment proposes that Fourth Amendment doctrine at the border should apply use-restrictions to properly balance individual privacy against the government's deep national security interests.

This Comment addresses the splintering doctrine between the First, Fourth, Ninth, and Eleventh Circuits regarding the Fourth Amendment limitations to performing forensic electronic searches at the border. Use restrictions consider each use of data—extracting, retaining, querying, and sharing—as a separate Fourth Amendment search, subject to a separate reasonableness analysis. This Comment will argue that applying such restrictions in the border context prevents the government from using data collected under a narrow exception for broader purposes that would otherwise require a warrant.

[†] B.A., The Georgia Institute of Technology, 2019; J.D. Candidate, The University of Chicago Law School 2025. My sincere thanks to Professor McAdams for his command of the relevant legal scholarship and guidance during the writing process, along with the staff of *The University of Chicago Legal Forum* for their hard work and editorial support and especially Eva Nobel, who gave critical feedback that made this comment possible and emotional support that allowed its writer to complete it.

I. INTRODUCTION

Border Protection Agents enjoy almost unfettered discretion to confiscate a person's belongings. This is because border searches constitute an exception to the Fourth Amendment's requirement that government officials generally must obtain a warrant before conducting a search. Under the exception, courts permit, without any level of suspicion, full searches of mobile living quarters;[1] the dismantling of car gas tanks;[2] and, in southern states from Texas to Florida, the highly intrusive copying of cell phone data.[3] The power is not only wielded against foreigners. Any international traveler to or from the United States, citizen or non-citizen, faces the risk of forfeiting copies of all locally-stored personal data.

This overreach into the data of citizens and noncitizens should prompt concern even among those who have nothing to hide. For example, following the U.S. National Security Agency's (NSA) expanded access to citizens' personal phone information, some NSA employees began "using secret government surveillance tools to spy on the emails or phone calls of their current or former spouses and lovers[.]"[4] United States Customs and Border Protection (CBP) similarly collects and retains highly sensitive data, like photographs and text messages, for up to fifteen years.[5]

The Fourth Amendment search and seizure doctrine on data collection practices is unsettled, especially in the border search context. Employees of the U.S. Department of Homeland Security (DHS)—which include people who work for U.S. Immigration and Customs Enforcement (ICE) and CBP—currently have full access to electronic device data from forensic border searches. Forensic electronic device searches can involve a breadth of activities.[6] This Comment uses the term 'forensic electronic device searches' to refer to border agents seizing an electronic device, extracting all the locally stored data, copying it to a

---

[1] *See, e.g.*, United States v. Alfaro-Moncada, 607 F.3d 720, 732 (11th Cir. 2010).

[2] *See, e.g.*, United States v. Flores-Montano, 541 U.S. 149, 155 (2004).

[3] *See, e.g.,* United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018).

[4] *See* Alina Selyukh, *NSA Staff Used Spy Tools on Spouses, Ex-lovers: Watchdog*, REUTERS (Sep. 27, 2013), https://www.reuters.com/article/idUSBRE98Q14H/ [https://perma.cc/P4PT-UXW8]. Congress has since implemented statutory restrictions to limit this practice and other intrusions into U.S. person's privacy. *See* Brittany Adams, *Striking a Balance: Privacy and National Security in Section 702 U.S. Person Queries*, 94 WASH. L. REV. 401, 405 (2019).

[5] Letter from Troy Miller, Acting Comm'r of U.S. CBP to Sen. Ron Wyden, at 2 (Jan. 24, 2023) [hereinafter CBP Letter].

[6] *See* United States v. Cano, 934 F.3d 1002, 1008–09 (9th Cir. 2019) (distinguishing between a "manual search of a cell phone" where an agent browsed the call log and wrote down information stored on it versus a "forensic cell phone search" where the agent used a software to download all data stored locally on the phone).

database, and retaining it for future use, such as analysis, queries, or sharing. At least some travelers are selected at random for electronic searches.[7]

This Comment argues that CBP's electronic device search policy violates the Fourth Amendment because it fails to consider suspicion requirements for reasonable use of data after retention. In 2017, CBP conducted 30,200 electronic device searches without any requirement for probable cause or reasonable suspicion.[8] The following year, CBP updated its internal collection policies to limit suspicionless searches.[9] Under the 2018 guidance, CBP officers may only conduct an "advanced" or forensic electronic search if reasonable suspicion exists. But CBP still annually processes over 40,000 travelers, along with their electronic devices, with limited suspicion and few judicial limits on use of the harvested data.[10] Because confused judicial interpretations of the Fourth Amendment fail to limit the use of traveler data to furthering border protection, the policy is expansive.

Through only modest adjustments to its internal policies of data usage after collection, CBP could easily comply with the Fourth Amendment. Such adjustments to its internal policies would not only more effectively protect the privacy interests of international travelers, but also give enforcement agencies the necessary flexibility to go after contraband and smugglers that endanger national security.

This Comment proposes that courts should limit CBP search and seizures of forensic electronic device data through use restrictions. The responsibility to outline a consistent national Fourth Amendment doctrine at the border that protects privacy falls on the courts. Because of confusion among the circuit courts of appeals regarding when a forensic electronic device search is reasonable, a traveler has different constitutional rights if they arrive at the Los Angeles International Airport in California or Miami International Airport in Florida.

Section II explains how courts have interpreted the border exception to provide more leeway for searches and seizures by government agents despite a lack of articulable, individualized suspicion because of the great governmental interest in protecting the border. Section III

---

[7] *See, e.g.*, *id.* at 1008.

[8] *See CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, U.S. CUSTOMS AND BORDER PROT. (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and [https://perma.cc/7R89-GMF4].

[9] DEPT. OF HOMELAND SEC., U.S. CBP DIRECTIVE 3340-049A.2.3, BORDER SEARCH OF ELECTRONIC DEVICES 5 (2018) [hereinafter 2018 CBP Directive re Border Search of Electronic Devices].

[10] *See CBP Enforcement Statistics*, U.S. CUSTOMS AND BORDER PROT. (Apr. 17, 2024), https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics [https://perma.cc/A7ZT-WF65].

explains the doctrinal hooks of use restrictions and how they have been applied across courts, particularly in the context of Fourth Amendment exceptions, which are intended to be applied in narrow circumstances. Section IV details two circuit splits in border exception doctrine with respect to forensic electronic device searches. The First and Fourth Circuits disagree with the Ninth and Eleventh Circuits over whether the underlying purpose of the border exception is limited to only the historic purpose of preventing contraband or has expanded to include searches for evidence of contraband. The Fourth and Ninth Circuits diverged with the Eleventh Circuit on the level of suspicion required to reasonably perform a forensic electronic device search following *Riley v. California*, which requires a warrant for police to lawfully conduct forensic electronic searches.[11] Section V proposes a use restriction framework to reconcile discrepancies across courts by analyzing different data usages as separate searches and seizures subject to separate reasonableness analyses.

This Comment argues that the Fourth Amendment establishes more heightened protections for travelers' data than have been recognized in much of the border search case law. Courts should treat the extraction, retention, and querying or sharing of stored electronic device data as separate searches. This practice would simultaneously reconcile the divergence in circuits' border search exception doctrine, protect travelers' privacy, and still provide border agents necessary tools to protect national security interests at the border.

II. PRIVACY PROTECTIONS FOR BORDER SEARCHES

A. Fourth Amendment Doctrine Protects Against Unreasonable Searches by Weighing the Intrusion on an Individual's Privacy Against the Government's Interest

As the Supreme Court has counseled, "[t]he Fourth Amendment commands that searches and seizures be reasonable. What is reasonable depends upon all the circumstances surrounding the search or seizure and the nature of the search or seizure itself."[12] Thus, the Fourth Amendment protects only against *unreasonable* searches and seizures. Courts determine whether a particular search or seizure is reasonable through a balancing test, weighing the "intrusion on the individual's

[11] 573 U.S. 373, 402 (2014) (holding that the exigent circumstances exception to warrant requirement does not extend to forensic electronic searches).

[12] United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).

Fourth Amendment [privacy] interests against its promotion of legitimate governmental interests."[13]

The Court requires an officer to articulate differing levels of suspicion to establish sufficient government interest to perform a reasonable Fourth Amendment search. External circumstances, like officer safety or the possible destruction of evidence, can increase the governmental interest, and thus decrease the level of suspicion needed for a search to be reasonable.[14] The Supreme Court generally holds that warrantless searches not based probable cause are "per se unreasonable," barring a "few specifically established and well-delineated exceptions."[15]

Probable cause can be established by demonstrating "a fair probability that contraband or evidence of a crime will be found."[16] However, the Supreme Court has allowed for certain Fourth Amendment exceptions, wherein an officer may conduct a search with little or no cause for suspicion. For example, a "brief investigative traffic stop" implicates considerable government interests and thus may be conducted with only reasonable suspicion.[17] The Supreme Court has stated that "[a]rticulating precisely what 'reasonable suspicion' and 'probable cause' mean is not possible."[18] But reasonable suspicion is a "less demanding standard than probable cause and requires a showing considerably less than preponderance of the evidence."[19] It is based on the totality of circumstances and is not "readily, or even usefully, reduced to a neat set of legal rules,"[20] but also demands more than an "inchoate or unparticularized suspicion or hunch."[21] No suspicion is the lowest level. It is sufficient to perform a search only when government interest is already so high that no suspicion is required for the search to be reasonable.

One exception to the Fourth Amendment's general requirement that government officials must demonstrate probable cause and obtain a warrant before searching an individual exists in the border search context. The level of suspicion required for a search at the border is substantially lower than probable cause, though it differs for routine or nonroutine searches. First, to perform a routine search government

---

[13] United States v. Villamonte-Marquez, 462 U.S. 579, 588 (1983).

[14] *See*, *e.g.*, Arizona v. Gant, 556 U.S. 332, 346–47 (2009) (discussing when officers may not require a warrant to conduct a reasonable search "when safety or evidentiary concerns demand").

[15] Katz v. United States, 389 U.S. 347, 357 (1967).

[16] Illinois v. Gates, 462 U.S. 213, 238 (1983).

[17] Kansas v. Glover, 589 U.S. 376, 380 (2020).

[18] Ornelas v. United States, 517 U.S. 690, 695 (1996).

[19] *Id.* at 696.

[20] *E.g.*, United States v. Sokolow, 490 U.S. 1, 7–8 (1989) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

[21] Terry v. Ohio, 392 U.S. 1, 30 (1968).

agents need not establish any individualized suspicion. Indeed, they may even choose to search individuals at random. Alternatively, non-routine searches, which may be highly intrusive, require only that an officer hold a reasonable suspicion of lawbreaking activity. Although the border exception establishes a lower level of suspicion than other exceptions for routine searches, non-routine searches may only be conducted with reasonable suspicion.

In a series of cases, the Warren Court shifted Fourth Amendment doctrine from one intended to protect citizens' property rights to one intended to defend expectations of privacy.[22] Whereas before, the government could only seize personal property when it had a greater possessory interest than the owner, now it may seize property pursuant to the privacy balancing test.[23] Under the current doctrine, the government does not have possessory interest in the items it seizes, which means it may not use the property with the same free reign as a true owner.[24] The border exception must also respect individuals' reasonable expectations of privacy.[25] Thus, even personal property seized using the border exception is still subject to Fourth Amendment limitations protecting individual privacy.

B. The Border Exception's Historic Origins

The Supreme Court acknowledges that Congress delegated the executive "plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant."[26] This immensurable authority, known as the border exception, is rooted in "the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country."[27] To establish this longstanding right, the Supreme Court pointed to the First Congress' first customs act, the Tariff Act of 1789 (the "Tariff Act"), which "granted customs officials 'the full power and authority' to enter and search 'any ship or vessel, in which they shall have reason to suspect

---

[22] *See* Katz v. United States, 389 U.S. 347, 352 (1967) (protecting privacy to talk from a public phone booth); Mancusi v. DeFort, 392 U.S. 364, 369 (1968) (protecting privacy to store records in areas available to employers); Minnesota v. Olson, 495 U.S. 91, 100 (1990) (protecting privacy to stay overnight in a friend's apartment, holding that "[w]e need go no further than to conclude, as we do, that Olson's status as an overnight guest is alone enough to show that he had an expectation of privacy in the home").

[23] *See Katz*, 389 U.S. 347, 359 (1967) (Harlan, J. concurring); William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1017 (1995) (discussing effects of adopting privacy as the focus of Fourth Amendment law); Harold Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 54–60 (1995).

[24] *See* Krent, *supra* note 23, at 54.

[25] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 540 (1985).

[26] *Id.* at 537.

[27] United States v. Ramsey, 431 U.S. 606, 616 (1977).

any goods, wares or merchandise subject to duty shall be concealed.'"[28] The Tariff Act only permitted searches if they were seeking contraband.[29] Border searches are "an old practice and [are] intimately associated with excluding illegal articles from the country."[30]

Although courts leverage different rationales to justify the border exception,[31] all courts recognize that the "longstanding right of the sovereign to protect itself" at the border factors heavily when courts perform Fourth Amendment privacy balancing tests.[32] At the border, the balance between an individual's privacy interests and the governmental interests "are struck much more favorably to the Government."[33] Since before the adoption of the Fourth Amendment, border searches have been considered reasonable "by the single fact that the person or item in question entered into our country [the United States] from outside."[34] This authority applies equally to those entering or exiting the country.[35]

C. Limits to Justifying Searches Under the Border Exception

The law places two modest but important limits to the border exception. First, nonroutine searches require reasonable suspicion. In other words, searches that are highly intrusive to individual privacy may not be conducted unless border agents ascertain reasonable suspicion of violation of a border crime. Second, the search itself must be restricted to items within the purpose of the exception that establishes the government's interest, or the search must relate to protecting the border.[36]

---

[28] *Id.* (citing Tariff Act of 1789, 1 Stat. 24).

[29] *See id.* at 617 (quoting Boyd v. United States, 116 U.S. 616, 623 (1886) ("The seizure of stolen goods is authorized by the common law; and the seizure of goods forfeited for a breach of the revenue laws, or concealed to avoid the duties payable on them, has been authorized by English statutes for at least two centuries past, and the like seizures have been authorized by our own revenue acts from the commencement of the government.").

[30] United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971).

[31] For example, *Ramsey* points to historical underpinnings, *see* 431 U.S. at 616-18, while *Montoya de Hernandez* notes the U.S. government's high interest in preventing anything harmful from entering such as "communicable diseases, narcotics, or explosives." 473 U.S. 531, 544 (1985).

[32] *See* United States v. Flores-Montano, 541 U.S. 149, 152, 154 (2004).

[33] *Montoya de Hernandez*, 473 U.S. at 540.

[34] *Ramsey*, 431 U.S. at 619.

[35] *See*, *e.g.*, United States v. Boumelhem, 339 F.3d 414, 422–23 (6th Cir. 2003); United States v. Odutayo, 406 F.3d 386, 391–92 (5th Cir. 2005); United States v. Oriakhi, 57 F.3d 1290, 1296–97 (4th Cir. 1995); United States v. Ezeiruaku, 936 F.2d 136, 143 (3d Cir. 1991); United States v. Cardona, 769 F.2d 625, 629 (9th Cir. 1985); United States v. Udofot, 711 F.2d 831, 839–40 (8th Cir. 1983).

[36] United States v. Kolsuz, 890 F.3d 133, 143 (4th Cir. 2018) ("[T]he scope of a warrant exception should be defined by its justifications.").

1. Routine versus nonroutine searches

Routine searches of a person and their effects are "not subject to any requirement of reasonable suspicion, probable, cause or warrant."[37] Nonroutine searches are subject to a higher individualized "reasonable suspicion" standard.[38] In other words, a nonroutine search may only be conducted if the agent conducting the search has a reasonable suspicion that the individual being searched is committing an activity the exception is intended to prevent.

A search becomes nonroutine when it goes "beyond the scope of a routine customs search and inspection"[39] and becomes highly intrusive, implicating "dignity and privacy interests the person being searched."[40] These include, but are not necessarily limited to, "strip, body cavity, or involuntary x-ray searches."[41] The Supreme Court in *Riley* held that forensic searches of cell phone data are also highly intrusive, nonroutine searches because the "sum of an individual's private life can be reconstructed" with the device's stored data.[42]

2. Border searches must further a purpose of the border exception

The purpose of a Fourth Amendment exception "define[s] the boundaries of the exception."[43] If the purpose of a search becomes too attenuated from the purpose of the exception, it cannot leverage a lower level of suspicion by veiling it as a border search. Instead, the evidence must be subjected to the classic Fourth Amendment test of balancing the government's interest against an individual's personal expectations of privacy.

In *Arizona v. Gant*, the Supreme Court used this principle to decline to extend the search incident to arrest exception.[44] Searches incident to arrest are permitted without suspicion to "protect[] arresting officers and safeguard[] any evidence of the offense of arrest that an arrestee might conceal or destroy."[45] For example, an officer may search

---

[37] *Flores-Montano*, 541 U.S. at 153 (citing *Montoya de Hernandez*, 473 U.S. at 538).

[38] *See* United States v. Cano, 934 F.3d 1002, 1012 (9th Cir. 2019); *Kolsuz*, 890 F.3d at 139; United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018); *Montoya de Hernandez*, 473 U.S. at 541.

[39] *Montoya de Hernandez*, 473 U.S. at 541.

[40] *Flores-Montano*, 541 U.S. at 152.

[41] *Montoya de Hernandez*, 473 U.S. at 541 n.4.

[42] Riley v. California, 573 U.S. 373, 394 (2014).

[43] Arizona v. Gant, 556 U.S. 332, 339 (2009); *see also* Terry v. Ohio, 392 U.S. 1, 19 (1968) (quoting Warden v. Hayden, 387 U.S. 294, 310 (1967) ("The scope of the search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible.").

[44] 556 U.S. 332 (2009).

[45] *Id.* at 339.

to ascertain whether an arrestee has a gun. To retain fidelity to the underlying purposes of the search incident to arrest exception, the *Gant* Court limited an officer's ability to search a vehicle under the exception to when an arrestee "was within reaching distance of the passenger compartment," to protect officer safety, or "it was reasonable to believe the vehicle contains evidence of the offense," to safeguard evidence.[46]

Riley also litigated a violation of the search incident to arrest exception. The Supreme Court reiterated the exception's dual purposes of preventing "harm to officers and destruction of evidence," from prior precedents.[47] *Riley* found that while these risks were necessarily present in "the context of physical objects" it could not be extended to conduct forensic cell phone searches because "[t]here are no comparable risks when the search is of digital data."[48] *Riley* held that "officers must generally secure a warrant before conducting" forensic cell phone searches.[49]

In the border context, a search at the border for "general law enforcement purposes" might still be reasonable considering reduced expectations at the border, but the analysis depends on the factual circumstances. For example, in *United States v. Soto-Soto*,[50] an FBI agent's suspicionless search of a vehicle crossing the border for "general law enforcement purposes," specifically to check if the car was stolen, was considered outside the scope of the border exception.[51] The *Soto-Soto* court excluded the evidence on the ground that Congress had not delegated authority to the FBI to conduct border searches, instead restricting that authority to other agencies.[52] The *Soto-Soto* Court stated it would not reach the "expectation of privacy" constitutional balancing test because the search was represented a statutory violation.[53]

3. Circuits are divided in reading the purpose of the border exception

The Supreme Court established two principal purposes for the border exception: (1) to identify "[t]ravelers . . . entitled to come in" and (2) to verify their "belongings as effects which may be lawfully brought

---

[46] *Id.* at 351.

[47] *Riley*, 573 U.S. at 386.

[48] *Id.*

[49] *Id.*

[50] 598 F.2d 545, 549 (9th Cir. 1979).

[51] *Id.*

[52] *Id.*

[53] *Id.* at 550.

in."[54] However, the Circuit Courts of Appeals are split as to what kinds of searches fit under these purposes.

The Ninth Circuit adopts the narrowest version of the border exception's purpose: only border enforcement agents may invoke the exception, and they may only do so to stop contraband from entering the United States.[55] Discerning purpose of the border exception was a central issue in *United States v. Cano*.[56] Ultimately, the Ninth Circuit held that while the border exception can be leveraged to prevent contraband, it cannot be used to search for evidence of non-border-related crimes nor for "evidence of past or future border-related crimes."[57] For example, child pornography qualifies as digital contraband within purpose of the border exception, but emails evincing a price-fixing conspiracy fall outside the exception.[58] *Cano* points to history to make the point. It cites Supreme Court precedent showing "'[d]etection of . . . contraband is the strongest historic rationale for the border search," and recounts that all Supreme Court border search cases involved "items being smuggled."[59]

Even under this view, general law enforcement searches could be conducted at the border, but only if the government can establish a sufficient interest to outweigh individual privacy interests under the Fourth Amendment balancing test for interior searches. In other words, the Ninth Circuit prohibits general law enforcement searches at the border from leveraging the lower suspicion requirements of border searches.[60]

Some critique this expressed purpose as too narrow. One recently published comment argues that the border exception should also exempt the probable cause and warrant requirement for transnational criminal investigations in addition to the longstanding, historic purpose

---

[54] Carroll v. United States, 267 U.S. 132, 154 (1925); *see also* Laura K. Donohue, *Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 YALE L.J.F. 961 (2019); United States v. Ramsey, 431 U.S. 606, 620 (1977) ("The border search exception is grounded in the right of the sovereign to control who and what may enter the country."); United States v. Cotterman, 709 F.3d 952, 960 (9th Cir. 2013) (noting that border searches are generally deemed reasonable when they occur at the border because the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border") (citing United States v. Flores-Montano, 541 U.S. 149, 152 (2004)).

[55] *See* United States v. Cano, 934 F.3d 1002, 1013 (9th Cir. 2019).

[56] *Id.* at 1016–17.

[57] *Id.* at 1017 (holding the border exception may not be used to "conduct a search for evidence that [the suspect] was involved in sex-crimes generally" nor to "search for evidence of past or future border-related crimes").

[58] *See id.*

[59] *See id.* at 1018.

[60] Other circuits have misplaced concerns that the Ninth Circuit law would prevent border agents from any search related to crimes outside the border exception's purpose. *See* United States v. Haitao Xiang, 67 F.4th 895, 900 (8th Cir. 2023).

of preventing contraband.[61] The comment points to *United States v. Aigbekaen* as an example of a court that properly applies the test.[62] There, the Fourth Circuit held that searches done to (1) protect national security, (2) block unwanted persons or effects, (3) regulate the collection of duties, or (4) prevent the introduction of contraband would all receive the lower suspicion requirements of border searches.[63]

The most extreme courts believe the border exception has no purpose-based limitation. The First Circuit in *Alasaad v. Mayorkas* acknowledged that searches using other Fourth Amendment exceptions must be limited in scope by their purpose, but refused to entertain the possibility that it also applied to the border exception.[64] Assuming for argument's sake that the restrictions did apply, *Alasaad* further held that border searches may be used to search for contraband but also "evidence of contraband, or evidence of activity in violation of the laws enforced or administered by CBP or ICE."[65] *Alasaad* does not go so far as to extend the border exception to cover a search for any general law enforcement purpose, however.

Despite disagreement on the underlying purpose of the border exception, all circuits agree that not all searches are reasonable just because they occur at the border. The border exception does not justify general law enforcement searches.[66] And while the Supreme Court has not clarified the purpose, it has only ever permitted suspicionless searches at the border because "the expectation of privacy is less at the border than the interior" and certain national security-related "governmental concerns," like exclusion of contraband, "are at their zenith at the border."[67]

Even assuming the border exception has a narrow purpose, it still has broad reach. It may be applied even if the search is "conducted at some physical or temporal remove"[68] and has long applied to searches conducted "at the physical border, functional equivalent of the border, or the extended border."[69]

---

[61] *See* Brenna Ferris, *Border Searches for Investigatory Purposes: Implementing a Border Nexus Standard*, 54 U. MICH. J. L. REFORM CAVEAT 1, 3, 16–17, 20 (2020).

[62] Ferris, *supra* note 61, at 19–20 (citing United States v. Aigbekaen, 943 F.3d 713, 721 (4th Cir. 2019)).

[63] *Aigbekaen*, 943 F.3d at 720.

[64] 988 F.3d 8, 19 (1st Cir. 2021).

[65] *Id.* at 21.

[66] *See Aigbekaen*, 943 F.3d at 721 (quoting United States v. Kolsuz, 890 F.3d 133, 143 (4th Cir. 2018)); United States v. Cano, 934 F.3d 1002, 1013 (9th Cir. 2019).

[67] *Aigbekaen*, 943 F.3d at 720 (quoting United States v. Flores-Montano, 541 U.S. 149, 152, 154 (2004)).

[68] *Kolsuz*, 890 F.3d at 142.

[69] 2018 CBP Directive re Border Search of Electronic Devices, *supra* note 9.

D. Modest Legislative and Administrative Protections from Border Searches

No statutes grant travelers additional rights against CBP border searches.[70] Through its silence, Congress has authorized CBP to establish administrative guidelines to conduct border searches to the maximum extent allowed by the Constitution.[71]

Administrative agencies like CBP "possess only the authority Congress has provided" by statute.[72] Of course, Congress cannot grant authority prohibited by the Constitution. CBP issued a *Directive on Border Search of Electronic Devices* to define how the agency will comply with the authorizing statutes and the constitution when conducting border searches.[73] Nonetheless, this directive is highly subject to changing political administration priorities. Thus, CBP may broaden the scope of forensic electronic device searches at the border by taking a broad view of the Constitution, a statute, or a directive.

The U.S. government has litigated on behalf of CBP agents in several circuits, advocating for considering forensic electronic device searches as routine searches. Because of this, CBP appears to side with constitutional interpretations that broaden the border exception's purpose and considers forensic electronic device searches as routine, since they consider electronic devices and the data as merely among "all types of personal property."[74]

1. CBP's electronic device border search policy

The Court recognizes the importance of self-imposed administrative checks in assessing the reasonableness of a search for Fourth Amendment purposes.[75] CBP abides by regulations outlined in its *Directive on Border Search of Electronic Devices*, which imposes more

---

[70] *See e.g.*, 8 U.S.C. § 1357(a) (limiting the power of immigration officers and employees to enter dwellings within twenty-five feet of the national border, without establishing similar limitations for travelers); HILLEL R. SMITH, CONG. RSCH. SERV., LSB10387, DO WARRANTLESS SEARCHES OF ELECTRONIC DEVICES AT THE BORDER VIOLATE THE FOURTH AMENDMENT? 6 (2021) (discussing two failed bills proposed in the 116th Congress which would have raised suspicion levels required to conduct manual and forensic electronic device searches and introduced a warrant requirement to access the digital content of an electronic device belonging to a U.S. citizen or lawful permanent resident).

[71] *See* 6 U.S.C. §§ 202, 211; 8 U.S.C. §§ 1225, 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d); 31 U.S.C. § 5317; 22 U.S.C. § 401.

[72] Nat'l Fed'n of Indep. Bus v. DOL, OSHA, 595 U.S. 109, 117 (2022).

[73] *See* 2018 CBP Directive re Border Search of Electronic Devices, *supra* note 9.

[74] *Id.*

[75] *See* United States v. Flores-Montano, 541 U.S. 149, 156 (2004) (Breyer, J. concurring) ("This administrative process should help minimize concerns that gas tank searches might be undertaken in an abusive manner."); Brittany Adams, *Striking a Balance: Privacy and National Security in Section 702 U.S. Person Queries*, 94 WASH L. REV. 401, 405 (2019).

stringent requirements for electronic searches than some circuits do.[76] This is an example of the CBP directive taking a broad view of the statue to preserve future legal arguments, but taking practical steps to limit agents from overreach to avoid litigation.

Under CBP's own directives, an officer may only extract data from an electronic device, i.e. "connect[] external equipment . . . to review, copy, and/or analyze its contents," if they have "reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern."[77] Such searches must be approved by supervisors classified as Grade 14 level or higher.[78] Officers are empowered to copy the information from the device upon "probable cause to believe that the device, or copy of the contents from the device, contains evidence of a violation of law that CBP is authorized to enforce or administer," [79] or if "the information relates to immigration, customs, or other enforcement matters."[80] Otherwise copies will be destroyed. The constitutionality of these provisions depends heavily on the underlying purpose of the border exception. CBP's "information related to" caveat firstly swallows the probable cause requirement, and secondly broadens the border exception's purpose beyond what any court has held.

All extractions and retentions must be documented and reported. However, once an item meets the above criteria, no limitations are imposed to the extent of data copied or stored.[81] Nor is there any limit on CBP's authority to share relevant, retained data with other agencies[82] or query it for other non-border related purposes later.[83]

2. CBP's practical application of the border search exception

CBP's internal policies empower agents to search through collected data from travelers to the maximum extent permitted by the Constitution. CBP currently collects, without a warrant, deeply personal data that is then "saved and searchable for 15 years by thousands of Department of Homeland Security (DHS) employees, with minimal protections against abuse."[84] When queries are made, the regulations require no

---

[76] *See* 2018 CBP Directive re Border Search of Electronic Devices, *supra* note 9.

[77] *Id.* at 5.1.4.

[78] *See id.*

[79] *Id.* at 5.5.1.1.

[80] *Id.* at 5.5.1.2.; U.S. CUSTOMS AND BORDER PATROL, BORDER SEARCH OF ELECTRONIC DEVICES TEAR SHEET CBP PUBLICATION NO. 3160-0423 (Apr. 2023) [hereinafter Tear Sheet].

[81] 2018 CBP Directive re Border Search of Electronic Devices, *supra* note 9.

[82] *Id.* at 5.5.1.3.

[83] *Id. passim*.

[84] Letter from Sen. Ron Wyden to Chris Magnus, Comm'r, U.S. Customs and Border

mechanism "to record the purpose of the search," ignoring an important administrative check used in other agency databases, like the FBI's.[85]

CBP argues that the practices fall within the guidelines set by "statutory and regulatory authorities, as well as applicable judicial precedent."[86] CBP emphasizes that forensic searches reach only information stored on the device, and "may not intentionally . . . access information that is solely stored remotely."[87] Critically, officers may collect and store data outside the scope of the purpose of the border exception to intercept contraband. This may include games, personal messages, pictures, and health data. CBP provides travelers an informative sheet outlining how CBP uses their data at some point during the forensic search, although not necessarily before it commences.[88] While CBP reports that its "[o]fficers use diverse factors to refer individuals for targeted examinations," the process for choosing who to target is clandestine.[89]

In *Alasaad*, the First Circuit upheld the CBP directive that guides forensic electronic searches regarding the suspicion requirement for extraction, as well as ICE's almost identical directive. The First Circuit did so by expanding the purpose of the border exception beyond "interdicting contraband," interpreting digital information to be in the same category as "communicable diseases, narcotics, or explosives."[90] Because the case involved a manual rather than forensic electronic device search, the *Alasaad* Court did not reach the question as to whether forensic searches were routine or nonroutine.[91]

CBP relies on *Flores-Montano*[92] to articulate its authority to conduct routine searches. CBP argues that its procedures go "above and

---

Protection, at 1 (Sep. 15, 2022).

[85] *Id.*; *see also* Glenn S. Gerstell, *How FBI Querying Under FISA Section 702 Works*, LAWFARE (July 10, 2023 8:00 AM) https://www.lawfaremedia.org/article/how-fbi-querying-under-fisa-section-702-works [https://perma.cc/YA3Q-X62W] ("As a result of the FISA Amendments Reauthorization Act of 2017, the FBI must obtain a specific order from the Foreign Intelligence Surveillance Court (FISC) before looking at the contents of communications in the 702 database where (a) the FBI used a search term pertaining to an American, (b) the FBI was searching for evidence of a domestic crime, but not foreign intelligence information, and (c) the search was for a predicated investigation for a domestic crime, not a national security matter. In simple terms, where the FBI is in effect investigating a particular American in a domestic criminal case, there should be extra protections, such as a court order, before the FBI may access the content of communications in the Section 702 database.").

[86] CBP Letter, *supra* note 5.

[87] *Id.* at 2.

[88] *See* Tear Sheet, s*upra* note 80.

[89] CBO Search Authority, U.S. Customs and Border Patrol, (June 30, 2023) [https://perma.cc/VP9Y-7CQ4].

[90] Alasaad v. Mayorkas, 988 F.3d 8, 20 (1st Cir. 2021).

[91] *See id.* at 19.

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

beyond" what is required by law.[93] In *Flores-Montano*, the Supreme Court held that CBP required no reasonable suspicion when an inspector "raised [a] car on hydraulic lift, loosened the straps and unscrewed the bolts holding the gas tank to the undercarriage of the vehicle, and then disconnected some hoses and electrical connections" before they "hammered off" adhesive material from the gas tank to search for drugs.[94] CBP appears to take the position that manually collecting cell phone data is merely another example of a routine search in part because of "the reduced expectation of privacy associated with international travel" and its allegation that courts have "rejected a categorical exception to the border search exception."[95]

CBP regulations allow officers to seize and manually search any cell phone data stored locally on an electronic device that crosses the border without suspicion.[96] An officer may extract cell phone data and query it upon reasonable suspicion of any "activity in violation of the laws enforced by CBP" or "a national security concern," which is far broader than any circuit's articulated purpose of the border exception.[97] This excludes data stored externally on a data cloud and not copied to local device storage.

Another internal check occurs at the copying stage. CBP will only retain copies of information obtained "(1) if there is probable cause to believe the information contains evidence of a violation of law that CBP is authorized to enforce or administer, or (2) if the information relates to immigration, customs, or other enforcement matters."[98]

Textually, the second requirement encompasses the first and is much broader than the specific scope of the border search exception. Although CBP is currently reassessing how long it will retain data, as of now, the agency retains copied data for fifteen years.[99] CBP, without oversight, alleges it "will consider the appropriate balance of privacy safeguards and operational mission requirements in this assessment."[100]

---

[93] *See* 2018 CBP Directive re Border Search of Electronic Devices, *supra* note 9.

[94] *Flores-Montano*, 541 U.S. at 151–153 (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977) ("[S]earches 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 they occur at the border.")).

[95] *See* 2018 CBP Directive re Border Search of Electronic Devices, *supra* note 9 ("[L]ongstanding federal court precedent recognizing the constitutional authority of the U.S. government to conduct border searches . . . authorize[s] CBP to inspect and examine . . . all types of personal property, including electronic devices.").

[96] *See* 2018 CBP Directive re Border Search of Electronic Devices, *supra* note 9.

[97] *Id.* at 5.4.1.

[98] CBP Letter, *supra* note 5.

[99] *Id.* at 2.

[100] *Id.*

CBP implements nominal administrative checks for querying the data it collects. To have access to the database, "users must undergo annual security and data privacy training and obtain approval from CBP management and the [Automated Targeting System (ATS)] system owner before gaining access to ATS for official purposes."[101] ATS, which is a contracted Privacy Act-compliant third-party data storage system, "performs extensive auditing that records the search activities for all users."[102] Furthermore, CBP limits access to information in ATS to "personnel who have a need-to-know the information for their official government duties."[103]

CBP shares this information broadly. In other contexts, such as the Interagency Border Inspection System, CBP officers share information with twenty other federal agencies or bureaus, including the Internal Revenue Service, Secret Service, and Federal Bureau of Investigation, to determine how to target individuals for secondary examination upon arrival in the U.S.[104] Additionally, the tear sheet provided to individuals subjected to manual or forensic electronic searches indicates that "the information obtained during the course of this search may be made available to other agencies if CBP determines there is a need for further investigation, to obtain assistance such as subject matter expertise, translation assistance, decryption, or other technical assistance."[105]

III. USE RESTRICTIONS AS LIMITS TO FOURTH AMENDMENT DATA SEARCHES

The evolution of technology brings a new idea to the forefront: "what the government does with the information may now threaten privacy more than the collection itself."[106] Whereas the government is required to return property to an owner after a legitimate seizure (unless it is contraband), copies of data that were seized during a search present a gray space that courts have not yet definitively determined how to resolve.[107]

Still, objective "Founding-era understandings" of expectations of privacy inform courts "when applying the Fourth Amendment to innovations in surveillance tools."[108] The "privacy interests at stake in

---

[101] *Id.* at 3.

[102] *Id.*

[103] *Id.*

[104] *See CBO Search Authority*, U.S. CUSTOMS AND BORDER PATROL (June 30, 2023) [https://perma.cc/VP9Y-7CQ4].

[105] Tear Sheet, *supra* note 80.

[106] *See* Krent, *supra* note 23, at 52.

[107] *See id.* at 52–53.

[108] Carpenter v. United States, 585 U.S. 296, 305 (2018).

duplicat[ing]" private data imply use restrictions on government seizures.[109] This Comment will build on existing scholarship to apply use restrictions to the border exception context by showing that data extraction, retention, and querying or otherwise using are separate Fourth Amendment inquiries, and thus require individualized balancing tests.[110]

A. Doctrinal Underpinnings of Use Restrictions

Use restrictions are broadly defined as legal restrictions "constraining what law enforcement officials do with information already in their possession."[111] The idea of use restrictions as a method to constrain law enforcement searches was first proposed by Harold Krent in 1995,[112] who focused on applying use restrictions to DNA databases.[113] Krent argues that when a court holds that a search is reasonable, "they are sanctioning the government's seizure of the evidence for the articulated purpose."[114] The case for use restrictions is doctrinally the strongest in the context of Fourth Amendment exceptions. This is because the minimal suspicion required for the search is predicated on a strictly limited purposes.[115] Were the same search performed for a lesser purpose, the balance of reasonable privacy expectations against government interests would no longer tilt to the same side.[116] Thus, logically, the U.S. government is restricted from using extracted data in a way running contrary to the purpose of the extraction.

For example, in *National Treasury Employees Union v. Von Raab*,[117] the Court held that a government employer collecting and testing employee urine samples was reasonable under the Fourth Amendment in part because they would not be used for criminal prosecution.[118] Had the government later turned around and shared the samples with the police, the collection would likely no longer be reasonable. The border exception is a particularly good fit for use restrictions because the exception itself has a limited purpose.

---

[109] Note, *Digital Duplications and the Fourth Amendment*, 129 HARV. L. REV. 1046, 1049 (2016).

[110] *See id.*

[111] Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 137 (2017).

[112] *See* Krent, *supra* note 23, at 50.

[113] *See id.* at 86–87.

[114] *Id.* at 64.

[115] *See* Simmons, *supra* note 111, at 143.

[116] *See e.g.*, Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665 (1989) (emphasizing interest balancing and the program's underlying purpose when analyzing special governmental need searches).

[117] 489 U.S. 656 (1989).

[118] *See id.* at 667–68.

While the Supreme Court has not formally adopted use restrictions, they are permissible under current doctrine.[119] Furthermore, in *Maryland v. King*,[120] the Supreme Court itself implicitly endorsed use restrictions. It found that "if in the future police analyze [DNA] samples" that were collected to identify perpetrators for other purposes such as disease detection, that future analysis would implicate additional privacy concerns. A growing number of lower courts have turned "to use restrictions to solve some of the modern problems posed by technology and the Fourth Amendment."[121]

B. Different Forms of Use Restrictions

Use restrictions can take different forms. Krent advocated categorical bans on any data usage not disclosed before the original collection.[122] Other scholars propose that courts limit government searches by noting "a series of small seizures . . . conceptually distinct from . . . the seizure" as a whole.[123] This concept of separate seizures has previously been applied to the data context by scholars differentiating data extraction from "the uses law enforcement authorities make" of extracted information.[124]

In the border exception context, separate seizures should apply at the extraction, retention, and use (which could involve querying or sharing) stages. At each stage, a separate balancing test should be applied.

---

[119] Both the Supreme Court and several appellate courts have implicitly separated uses of data when analyzing Fourth Amendment searches. In *Lindell v. United States*, the Eight Circuit separated the retention of data, finding that "absent sufficient justification, the government has no right to hold onto property that is not contraband indefinitely," even if lawfully seized. 82 F.4th 614, 621 (8th Cir. 2023) (citing United States v. Premises Known as 608 Taylor Ave., Apartment 302, Pittsburgh, Pa., 584 F.2d 1297, 1302 (3d Cir. 1978)). In *Carpenter v. United States*, the Court found that government use of public data was a search. 585 U.S. 296, 316 (2018). In *United States v. Jones*, the Court held that GPS data could not be used "indefinitely for evidentiary searches." 565 U.S. 400, 404 (2012); *Id.* at 413 (Sotomayor, J. concurring). In *Skinner v. Railway Labor Executives' Ass'n*, the Court found that further analysis of lawfully acquired samples constituted a separate search. 489 U.S. 602, 616-17 (1989) ("The ensuing chemical analysis of the sample to obtain physiological data is a further invasion of the tested employee's privacy interests. . . . It is not disputed . . . that chemical analysis of urine, like that of blood, can reveal a host of private medical facts about an employee, including whether he or she is epileptic, pregnant, or diabetic."). And most notably in *Riley v. California*, the court held that forensic cell phone searches were separate from other related seizures and thus subjected to a higher standard of review. Riley v. California, 573 U.S. 373, 386 (2014).

[120] 569 U.S. 435, 464–65 (2013).

[121] Simmons, *supra* note 111, at 180; *see, e.g.*, United States v. Ganias, 755 F.3d 125, 137 (2d Cir. 2014) (restricting the use of digital data once it was in the possession of law enforcement).

[122] *See* Krent, *supra* note 23, at 53.

[123] Jim Harper, *Administering the Fourth Amendment in a Digital Age*, NAT'L CONST. CTR., https://constitutioncenter.org/news-debate/special-projects/digital-privacy/the-fourth-amendment-in-the-digital-age [https://perma.cc/PLW7-GKTJ] (citing South Dakota v. Opperman, 428 U.S. 364, 376 (1976)).

[124] *See* Krent, *supra* note 23, at 51.

Information acquired under the border exception for the purpose of preventing its entry at the border cannot then be used for general law enforcement purposes except upon probable cause and a warrant.

IV. APPLYING THE BORDER EXCEPTION TO FORENSIC CELL PHONE SEARCHES

The First, Fourth, Ninth, and Eleventh Circuits disagree on how to determine when forensic electronic device searches fall into the border exception doctrine. All agree that a border search has never required more than reasonable suspicion.[125] While courts generally agree that forensic electronic device searches might sometimes fall within the scope of the exception, they disagree as to whether the search is routine or nonroutine.[126] This distinction matters because it is the difference between whether CBP needs reasonable suspicion before conducting a forensic cell phone search or no suspicion at all.

In each border exception case, to determine if evidence should be excluded, a court must assess both (1) if the search is within the scope of the exception to discover contraband or to determine who is entering at the border and (2) whether the search was conducted with sufficient suspicion.[127]

The circuit cases applying this test have addressed different crimes. In the Ninth Circuit, Cano hid cocaine in the tires of his truck.[128] In the Eleventh Circuit, Touset smuggled child pornography on hard drives.[129] In the Fourth Circuit, Kolsuz dealt international arms.[130] The three fact patterns encompass physical contraband, digital contraband, and potential contraband. When assessing Fourth Amendment searches, facts matter to establish how to balance a person's privacy

---

[125] United States v. Wanjiku, 919 F.3d 472, 485 (7th Cir. 2019) ("[N]o circuit court, before or after *Riley*, has required more than reasonable suspicion for a border search of cell phones or electronically-stored data."); United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018) ("*Riley*, which involved the search incident to arrest exception, does not apply to searches at the border."); United States v. Molina-Isidoro, 884 F.3d 287, 291 (5th Cir. 2018) ("For border searches both routine and not, no case has required a warrant."); *id.* at 293 ("The bottom line is that only two of the many federal cases addressing border searches of electronic devices have ever required any level of suspicion. They both required only reasonable suspicion and that was for the more intrusive forensic search."); *see also* United States v. Kolsuz, 890 F.3d 133, 137 (4th Cir. 2018) (concluding that a "forensic examination of Kolsuz's phone must be considered a nonroutine border search, requiring some measure of individualized suspicion" but declining to decide whether the standard should be reasonable suspicion or probable cause).

[126] *See* United States v. Cano, 934 F.3d 1002, 1007 (9th Cir. 2019); *Kolsuz*, 890 F.3d at 137. *But see Touset*, 890 F.3d at 1233.

[127] *See Cano*, 934 F.3d at 1012; *see also* Ferris, *supra*, note 49 at 9.

[128] *See Cano*, 934 F.3d at 1008.

[129] *See Touset*, 890 F.3d at 1230.

[130] *See Kolsuz*, 890 F.3d at 138.

against the government's interest, particularly for Fourth Amendment exceptions.

A. Are Forensic Electronic Device Searches Within the Scope of the Border Exception?

Courts read the scope of the border exception to reach beyond ordinary border crossings. Border searches may be conducted at a "temporal and spatial distance" from the attempted entry.[131] Additionally, all courts agree that digital contraband, such as child pornography, puts at least certain forensic electronic device searches with the scope of the exception.[132] But beyond that agreement, the courts begin to splinter over what types of forensic searches fall within the exception.

Courts disagree as to whether the border exception applies when agents search for evidence of contraband as opposed to contraband itself. While the Ninth Circuit found the border exception must be directed toward discovering contraband,[133] the Fourth Circuit found the border exception also encompasses searches for evidence of future contraband.[134] The First Circuit is perhaps even more permissive, allowing the border exception to reach any "evidence of activity in violation of the laws enforced or administered by CBP or ICE."[135] The Ninth and First Circuits respectively represent the lower and upper bounds of the scope of the border exception. Quoting *Boyd v. United States*,[136] the Ninth Circuit in *Cano* reiterated that "the search for and seizure of stolen" goods as "totally different [] from a search for and seizure of [goods] . . . for the purpose of obtaining information therein contained, or of using them as evidence against him. The two things differ *toto coelo*."[137]

The Fourth and First Circuits take the broadest view of the scope of border searches with respect to forensic electronic device searches. These circuits hold that the border exception encompasses searches conducted when persons seek to "depart the country," when a phone is in "government custody miles from the border," and even when there is a "month-long gap between" a person's border crossing and the search.[138]

---

[131] *Id.* at 137.

[132] *See, e.g.*, *Cano*, 934 F.3d at 1014 ("[Cell phone] data can contain digital contraband.").

[133] *See id.* at 1017.

[134] *Kolsuz*, 890 F.3d at 138.

[135] Alasaad v. Mayorkas, 988 F.3d 8, 21 (1st Cir. 2021).

[136] *Cano*, 934 F.3d at 1018 (quoting Boyd v. United States, 116 U.S. 616, 622–23 (1886)).

[137] *Id.*

[138] *Kolsuz*, 890 F.3d at 142; *see also*, United States v. Cotterman, 709 F.3d 952, 961–62 (9th Cir. 2013) (en banc) (applying border exception to forensic examination of laptop computer conducted miles from and days after attempted border crossing); United States v. Saboonchi, 990 F.Supp.2d 536, 548–49, 561 (S.D. Md. 2014) (applying border exception to forensic search of cell phones obtained at border with Canada but conducted several hundred miles away in Baltimore,

The Fourth Circuit held in *Kolsuz* that the "border search exception is broad enough to accommodate . . . the prevention and disruption of ongoing efforts to export contraband illegally."[139] Importantly, however, the court still acknowledged that at some point, "a search initiated at the border could become so attenuated from the rationale for the border search exception that it no longer would fall under that exception."[140]

In fact, the Fourth Circuit subsequently limited *Kolsuz*'s holding. In *Aigbekaen*, the Court held that border searches would not encompass all "general interest[s] in enforcing domestic criminal laws."[141] The First Circuit has not yet adopted a similar explicit limit, but it did exclude general law enforcement from its list of "full range of justification[s]."[142]

That CBP limits forensic searches to locally-stored data on the device undermines an interpretation of the border exception to encompass searches for mere evidence of contraband. If the border exception extends to other locations and times outside border crossings, it may reach data stored on the cloud as well, especially since data on the cloud would provide more evidence.[143] However, if the boundary of the exception is drawn at contraband, searches are limited to digital contraband that has physically crossed the border. Nonetheless, whether the border exception's purpose extends to collect mere evidence of any general crime remains an open question in the Fourth Circuit.[144]

The Eleventh Circuit is less direct in setting forward a clear rule of what falls within the border exception's scope. In *Touset*, the court justifies using the border exception by highlighting the First Congress' statute that allowed the search of "any vessel or cargo suspected of illegally entering the nation."[145] *Touset* holds that "border agents bear the

---

Maryland).

[139] *Kolsuz*, 890 F.3d at 143.

[140] *Id.* at 143 (citing United States v. Molina-Isidoro, 884 F.3d 287, 295–97 (Costa, J., concurring) (questioning whether search for evidence as opposed to contraband is consistent with justifications for border search exception)).

[141] 943 F.3d 713, 718 (4th Cir. 2019).

[142] Alasaad v. Mayorkas, 988 F.3d 8, 21 (1st Cir. 2021) ("Advanced border searches of electronic devices may be used to search for contraband, evidence of contraband, or for evidence of activity in violation of the laws enforced or administered by CBP or ICE.").

[143] *See* Nicolette Lotrionte, *The Sky's the Limit: The Border Search Doctrine and Cloud Computing*, 78 BROOK. L. REV. 663, 668 (2013).

[144] See *Molina-Isidoro*, 884 F.3d at 297 n.7 (5th Cir. 2018) (Costa, J., specially concurring) ("*Hayden* is viewed as a broad rejection of the 'mere evidence'/instrumentality distinction") (citing Wayne LaFave, *Search & Seizure, A Treatise on the Fourth Amendment* § 4.1(c)). *But see* Lotrionte, *supra* note 143 ("[T]here are reasons to believe the [mere evidence/instrumentality] distinction still matters when it comes to border searches.").

[145] United States v. Touset, 890 F.3d 1227, 1232 (11th Cir. 2018). The opinion also cites *Boyd* to show the First Congress did not regard searches and seizures of contraband as unreasonable. *Id.*

same responsibility for preventing the importation of contraband in a traveler's possession regardless of advances in technology."[146] This appears to be more aligned with the Ninth Circuit than the First and Fourth Circuits.

B. What Level of Suspicion is Required for Forensic Electronic Device Searches?

Circuits also disagree as to whether forensic electronic device searches are nonroutine and thus require reasonable suspicion. All circuits agree that, despite the *Riley* Court holding that "a warrant is generally required before such a search" of electronic data, the border search exception has never required more than reasonable suspicion for forensic electronic device searches.[147] Nonetheless, because *Riley* held that forensic electronic device searches are highly intrusive, circuits must determine whether these searches are routine or nonroutine in the border search context.[148]

The Eleventh Circuit takes a hardline approach, advocating that no search of any personal property, including electronic devices or digital data, can ever rise to a nonroutine search.[149] Meanwhile, the Ninth Circuit uses *Riley* to show that forensic electronic device searches are so highly intrusive as to require a higher level of suspicion before being conducted.[150] The Fourth Circuit agreed with the Ninth Circuit, in *Kolsuz*, holding "particularly in light of the Supreme Court's Decision in *Riley*, a forensic border search must be treated as nonroutine."[151] However, because the search still falls within the border exception, the Ninth and Fourth Circuits only raised the standard to "reasonable suspicion," instead of *Riley*'s warrant requirement.[152] As *Alassad* notes, "[e]very circuit that has faced this question" agrees there is no "warrant

---

[146] *Id.* at 1233.

[147] Riley v. United States, 573 U.S. 373, 401 (2014); *see also, e.g.*, *Molina-Isidoro*, 884 F.3d at 290 ("[T]he most demanding requirement a court has required for any type of border search is reasonable suspicion.").

[148] *See* Bingzi Hu, Esq., *Border Search in the Digital Era: Refashioning the Routine vs. Nonroutine Distinction for Electronic Device Searches*, 49 AM. J. CRIM. L. 177, 198 (2022) (arguing digital devices are qualitatively different from routine searches upsetting the balance of personal privacy versus significant government interests at the border).

[149] United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018); *see also* Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1093 (2009) ("This article argues that suspicionless border searches of laptop computers generally are permissible under the Fourth Amendment, but it importantly was written before *Riley*.").

[150] *See* United States v. Cano, 934 F.3d 1002, 1015 (9th Cir. 2019).

[151] United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018).

[152] *See id.* at 148; *Cano*, 934 F.3d at 1015.

requirement [under *Riley*] for border searches of electronic devices, whether basic or advanced."[153]

The Eleventh Circuit in *Touset* draws a firm line declaring "property and persons are different."[154] Acknowledging that *Flores-Montano* holds that nonroutine searches are subject to reasonable suspicion, the Eleventh Circuit also asserts that such nonroutine searches have only ever applied to "highly intrusive searches of a person's body."[155] Forensic electronic device searches do not implicate "(1) physical contact between the searcher and the person searched; (2) exposure of intimate body parts; and (3) use of force," which are the factors used to determine intrusiveness in the Eleventh Circuit.[156]

There are many reasons to be skeptical of *Touset*'s holding. First, while *Riley* applied a probable cause and warrant requirement for forensic cell phone searches, specifically in the searches incident to arrest exception, its description of a forensic cell phone search as highly intrusive applies to all Fourth Amendment exceptions.[157] Secondly, *Touset* found that the officer did have reasonable suspicion.[158] Thus, language resolving the standard for searches is merely dicta because it was not necessary to decide the issue before the court. *Touset* also avoids addressing *Flores-Montano*'s holding drawing a distinction between persons and property.[159] While it is true that *Flores-Montano* found that completely disassembling a fuel truck was a routine search, the Court also explicitly left open the possibility "that some searches of property are so destructive as to require a different result."[160] Although *Touset*'s treatment of *Riley* is suspect, its reasoning is somewhat bolstered by the long-standing "diminished privacy interest of travelers" weighed against the substantial "government[] interest in stopping contraband at the border."[161]

The Ninth and Fourth Circuits' reasoning is more straightforward. Recognizing the highly intrusive nature of a forensic electronic device search, the Courts found such a search is nonroutine, and thus requires reasonable suspicion to be conducted.[162]

---

[153] Alasaad v. Mayorkas, 988 F.3d 8, 17 (1st Cir. 2021).

[154] *Touset*, 890 F.3d at 1234.

[155] *Id.* (citing United States v. Alfaro-Moncada, 607 F.3d 720, 729 (11th Cir. 2010)).

[156] *Id.*

[157] *See* Riley v. California, 573 U.S. 373, 395 (2014).

[158] *Touset*, 890 F.3d at 1229.

[159] United States v. Flores-Montano, 541 U.S. 149, 155–56 (2004).

[160] *Id.* at 155.

[161] *Touset*, 890 F.3d at 1235.

[162] *See* United States v. Cano, 934 F.3d 1002, 1015 (9th Cir. 2019); United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018).

C. Use Restrictions Could Resolve Circuit Splits Regarding the Purpose and Suspicion Requirement for Forensic Electronic Device Border Searches

Although circuits are split on both the scope of and level of suspicion required for the border exception, analyzing the stages of forensic electronic device searches as separate searches may ameliorate discrepancies. In forensic cell phone searches, agents extract data through a downloading process, store the data for a period of time, then use the data, typically either by querying or sharing it. The cases above collapse these separate steps of a forensic cell phone search into one Fourth Amendment search. Instead, each step should be seen as a separate Fourth Amendment search with its own balancing test.

First, border agents can extract all data with no suspicion, regardless of whether it might fall under the scope of the border exception. This respects the Fourth and First Circuits' holdings on the border exception's broad purpose.

But, extracted data should only be queried if there is reasonable suspicion that such a query would return contraband. This would effectively respect *Riley's* holding that forensic searches are highly intrusive and the Ninth and Fourth Circuits' holding that a forensic electronic search is nonroutine. The data pulled from a query should only be stored if there is at least probable cause that it contains contraband. This properly honors the historically narrow purpose of the border exception limited to preventing contraband. Any querying, sharing, or otherwise using the stored data for evidence or other law enforcement purposes is outside the scope of the border exception and should undergo the traditional probable cause and warrant requirement.

Thus, the border exception provides few limits at the extraction stage, but as the dangers to an individual's sense of privacy become graver through the storage and use of the data, the restrictions become more serious. Separating forensic electronic device searches into steps of extraction, storage, and use upholds all Circuits' rationales.

V. APPLYING USE RESTRICTIONS TO THE BORDER SEARCH EXCEPTION

The Fourth Amendment's border exception should be interpreted such that forensic electronic device searches constitute at least three distinct searches, each requiring its own level of suspicion to establish reasonableness: (1) the extraction of data, (2) the retention of data, and (3) the querying and sharing of data. Such a scheme would ameliorate discrepancies between circuits, protect individual travelers' privacy interests, and still provide CBP the necessary flexibility to protect the border from unwanted items. While courts have traditionally demanded

only reasonable suspicion to justify invasive border searches, other precedents such as *Riley* should govern the scope and procedure of these searches as they diverge from the original scope of the border exception.

This section will explore how courts should balance governmental interests against individual privacy interests for forensic electronic searches at the border by applying use restrictions at the extraction, retention, and use stages. Part A argues that extracting data requires no reasonable suspicion so long as the search is narrowly confined to the purpose of the exception. However, CBP should only store extracted data upon confirmation or probable cause that contraband exists within it. Part B proposes that after data is extracted and retained, each additional use of that data constitutes a new search. Narrowly tailored queries for contraband require only reasonable suspicion, while queries for evidence or shares with other agencies requires a warrant upon probable cause. Finally, Part C shows that such a use-restriction regime for the border exception properly balances individual privacy with governmental interests, without compromising CBPs mission.

A. Extracting Data Requires No Suspicion Under the Border Exception While Storing Data Requires Probable Cause of Contraband

The first governmental use of an individual's data in a forensic electronic device search is extracting it. This is the least intrusive stage because mere extraction does not imply that anyone ever sees it, reviews it, or even stores it. Should use restrictions be applied to border searches, the government should still possess the authority to extract any data stored on an electronic device that could potentially contain digital contraband without any level of suspicion. This standard would respect both the *Touset* Court, which held that no suspicion was required for forensic electronic searches, and the Ninth and Fourth Circuits, which require at reasonable suspicion.[163] The standard would demonstrate that the Circuits were only mistaken by collapsing every step of a forensic electronic search into one.

This broad standard—"potentially contain"—is based on the court allowing almost all searches of physical property that may contain contraband.[164] Digital contraband is understood to include child pornography,[165] but might also include other things like copyright-infringing software. Digital contraband also has some clear limits; for instance, audio messages cannot contain digital contraband because words and communications alone are not illegal to import. Pictures, conversely,

---

[163] *See Touset*, 890 F.3d at 1236; *Cano*, 934 F.3d at 1017; *Kolsuz*, 890 F.3d at 140–41.

[164] *See Flores-Montano*, 541 U.S. at 154-55.

[165] *See Cano*, 934 F.3d at 1014 (discussing digital contraband).

may harbor digital contraband.[166] External factors, such as the duration of device confiscation, may introduce more substantial intrusions on reasonable expectations of privacy, warranting higher suspicion.[167]

Following extraction, the government must decide what data to store. Storage of personal data is highly intrusive to an individual's privacy. The data could be leaked, perused, or otherwise used without their knowledge. To establish a sufficient countervailing governmental interest, the government should only store actual digital contraband or data where probable cause of such contraband exists. This retained digital contraband, however, may be stored indefinitely subject to statutory regulations.[168]

B. Uses of Extracted and Stored Data Should Require No Suspicion for Querying Known Contraband, Reasonable Suspicion for Searching for Potential Contraband, and a Warrant Upon Probable Cause for Any Other Purposes

Under a use-restriction regime, different levels of suspicion should apply before an agent uses data depending on their intention. Querying data for known, stored digital contraband requires no suspicion, because this is undoubtedly within the purpose of the border exception. Searches for contraband do not implicate personal privacy interests, because smugglers have no expectations of privacy for illegal contraband.[169]

Querying data for evidence or to share data with other agencies should require a warrant upon probable cause because these are outside the scope of the border exception.[170] Of course, law enforcement could still use the data stored from the border exception to investigate general and border related crimes. But requiring probable cause ensures the

---

[166] *See Touset*, 890 F.2d at 1235.

[167] *See Kolsuz*, 890 F.3d at 141 ("Accordingly, we do not address whether and under what circumstances an extended confiscation of a traveler's phone—quite apart from any search undertaken—might constitute an unreasonable seizure of property for Fourth Amendment purposes.") (citing United States v. Saboonchi, 990 F.Supp.2d 536, 569 (S.D. Md. 2014) (noting that forensic searches of digital devices may "deprive individuals of their possessions for periods of days or weeks")).

[168] *See* Lindell v. United States, 82 F.4th 614, 621 (8th Cir. 2023) ("[A]bsent sufficient justification, the government has no right to hold onto property that is not contraband indefinitely) (citing United States v. Premises Known as 608 Taylor Ave., Apartment 302, Pittsburgh, Pa., 584 F.2d 1297, 1302 (3d Cir. 1978)).

[169] *See* Illinois v. Caballes, 543 U.S. 405, 408 (2005) ("We have held that any interest in possessing contraband cannot be deemed legitimate, and thus, governmental conduct that only reveals the possession of contraband compromises no legitimate privacy interest.") (cleaned up).

[170] *See Kolsuz*, 890 F.3d at 143 ("[W]here the government interests underlying a Fourth Amendment exception are not implicated by a certain type of search, and where the individual's privacy interests outweigh any ancillary governmental interests, the government must obtain a warrant based on probable cause.").

border exception is not misused through broad application. Warrants do not pose a significant hurdle to investigations related to data searches, since the data is already secured and there is low risk of loss of evidence.

To avoid implicating *Riley*'s assertion that electronic searches are highly intrusive and "typically expose to the government far *more* than the most exhaustive search of a house,"[171] querying extracted data in an initial search for contraband should require (1) reasonable suspicion that the data being queried contains digital contraband and (2) that the scope of the query be sufficiently limited to avoid discovering personal data. Reasonable suspicion is a good standard here because queries of personal data are nonroutine searches after *Riley*. Such queries require a tool unavailable to the public and dives deep into people's personal data.[172] Highly intrusive data is likely to yield personal information about a person's intimate activities such as location and communications,[173] not to mention potentially humiliating photographs or notes stored on the device.

Just as extraction requiring no suspicion satisfies the Eleventh Circuit, applying a reasonable suspicion requirement at the querying phase satisfies both the Ninth and Fourth Circuits' finding that forensic electronic searches are nonroutine. This is because a use-restriction regime merely shifts where the nonroutine search begins through the stages of a forensic electronic search. Requiring a warrant for data searches unrelated to the border exception's purpose, allows full fidelity to *Riley*.

C. CBP Compliance with a Use-Restriction Regime Does Not Compromise National Security

To abide by the proposed use-restriction based Fourth Amendment border exception framework, CBP must make modest adjustments to its procedures to comply. The most obvious is that it must narrow the purposes for which an agent may extract or copy data. CBP already requires changing levels of suspicion for extracting, copying, retention, and using electronic device data. However, the standards they place on each step, fail to map to the proposed framework.

---

[171] Riley v. California, 573 U.S. 373, 396; *see also id.* at 394 ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions.").

[172] *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).

[173] Harper, *supra* note 123 ("[I]t is part of human essence to have communications remain private."); *see also* United States v. Jones, 565 U.S. 400, 416 (2012) (Alito, J., concurring) (noting that GPS monitoring makes "available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track").

CBP currently employs a digital scraping tool to extract data from electronic devices.[174] This tool permits officers to select specific categories of data to be downloaded, for example only phone call data. CBP should create policies to differentiate which data might potentially contain contraband. Some types of data, like cell phone game data, contact lists, or voice messages, should never be extracted because none of these could contain forms of digital data that have been recognized by courts to be contraband. CBP cannot search data that does not potentially contain contraband without a warrant because it falls outside the scope of the border exception.[175]

CBP searches the vast amounts of data for contraband before retention primarily through queries. Queries should be a narrowly tailored search for contraband both in their wording but also in the scope of the data searched. Since queries are logged, courts can easily assess their narrowness. If incriminating information outside of contraband is uncovered during the process, it can be admitted as evidence under the plain view exception.[176] Defendants can also challenge queries as insufficiently narrow.[177]

Parties have successfully challenged query-searches in the past. *In re DNI/AG 702(h) Certifications 2018*[178] held that the FBI violated the Fourth Amendment because it did not comply with the statutory requirement to maintain a log of query terms and who conducted those searches.[179] The statute, which was designed by Congress to avoid Fourth Amendment concerns, "did not permit . . . run[ning] queries that were unlikely to return evidence of crime, even if they were subjectively intended to do so."[180] Courts have experience adjudicating these kinds of challenges to Fourth Amendment queries. Of course, CBP may make broader queries or search more data with a warrant upon probable cause.

---

[174] *See* United States v. Cano, 934 F.3d 1002, 1008 (9th Cir. 2019) (describing use of Cellebrite software); *Kolsuz*, 890 F.3d at 139 ("Cellebrite Physical Analyzer, which extracts data from electronic devices, and conducted an advanced logical file system extraction.").

[175] *See Kolsuz*, 890 F.3d at 143.

[176] The "plain view doctrine" authorizes the seizure of illegal or evidentiary items visible to a police officer whose access to the object has some prior Fourth Amendment justification and who has probable cause to suspect that the item relates to criminal activity. *See* Horton v. California, 496 U.S. 128, 142 (1990).

[177] Some courts have signaled a willingness to address the question of "what kinds of querying, subject to what limitations, under what procedures, are reasonable within the meaning of the Fourth Amendment" although have yet determine a test. *See* United States v. Hasbajrami, 945 F.3d 641, 672–73 (2d Cir. 2019).

[178] 941 F.3d 547, 559–560 (FISA Ct. Rev. 2019).

[179] *See id.*

[180] Redacted, 402 F. Supp. 3d 45, 83 (FISA 2018), *aff'd in part*, 941 F.3d 547 (FISA Ct. Rev. 2019).

D. Benefits to Shifting to a Use Restriction Analysis

From an administrative perspective, restricting separate uses of data as separate Fourth Amendment searches is more manageable for CBP. Agents would not need to explain any level of suspicion to extract data. Although agents would need to be trained to properly word narrow queries for contraband, once contraband is identified and stored it can be indefinitely retained. This eliminates the need to delete old or stale evidence and keeps personal data more secure from risk of hacking. Once an agent has identified and retained known digital contraband, it streamlines the administrative process for querying the database as no reasonable suspicion would be required to search for the retained contraband. Furthermore, since the contraband-data is secured, waiting for the process to get a warrant to share or search it for evidence poses low risk of losing evidence.

Congress, if it wishes, can extend CBP's enforcement authority to search for evidence of contraband, but "the dangers of judicial standard-setting in an area as sensitive as border searches [are] . . . apparent."[181] Adjudicating specific queries of specific data bases is exactly the realm for courts to balance the privacy interests of the person against the needs of the government.[182] Because queries are typically made using natural language, courts have expertise to determine if the query language is sufficiently narrow to be "reasonably designed to return" evidence within the purpose of the search.[183]

Some might argue that a use-restriction Fourth Amendment regime would hinder law enforcement's ability to protect the border. This concern is misplaced. In fact, a use-restriction regime would enhance CBP's ability to go after its chief targets, large-scale criminal cartels that smuggle drugs, weapons, and child pornography to the United States, by properly aligning incentives with the enforcement mechanisms.[184]

Large-scale criminal organizations are the travelers in the best position to avoid the risk related to carrying electronic devices with significant personal information. A smuggler who frequently goes in and out of the United States could simply carry two devices and have a

---

[181] United States v. Touset, 890 F.3d 1227, 1237 (11th Cir. 2018) (quoting United States v. Kolsuz, 890 F.3d 133, 151 (4th Cir. 2018).

[182] *See* United States. v. Villamonte-Marquez, 462 U.S. 579, 588 (1983).

[183] *Redacted*, 402 F. Supp at 83; *see also* 50 U.S.C. § 1801(h)(3) (dictating minimization procedures for electronic surveillance).

[184] *See e.g., CBP Announces Next Phase in Fight Targeting Criminals Funneling Fentanyl into America Communities*, U.S. Customs and Border Protection (Apr. 10, 2024) (announcing that CBP "will lead an expanded, multi-agency effort to target the transnational criminals . . . [that] targets cartels" that engage in "kidnapping, as well as the smuggling of humans, dangerous drugs, and firearms").

collaborator pick him up and drop him off from the airport or border. Likewise, if the purpose is to deliberately transport large quantities of digital contraband, a smuggler has no need to physically transport the data when it could be disguised in the mail.

Meanwhile, allowing invasive forensic electronic device searches with no suspicion requirement would put ordinary travelers at great discomfort in an already laborious traveling process. An ordinary person would not wipe their electronic device data before traveling just to redownload their data once they arrive at their next destination. And if they did not wipe their device data, then they might be subject to having their electronic devices confiscated and shipped to extraction areas across the country.

If we consider two alternatives to a use-restriction regime to address these problems, it is evident that both are unsatisfactory. First, if the Court read a broad purpose to the border search exception's scope to include evidence of contraband, it would incentivize avoidant behavior from cartels and chiefly intrude on the privacy of non-dangerous targets. The thrust of this proposal is that by giving CBP access to more data on an electronic device, they are more capable of discovering other smugglers in the network. It assumes a huge lack of sophistication among smuggler networks. They could easily change their behavior to store less data locally or not travel with electronics at all with minimal effect on their operations.

Furthermore, the travelers who would be most at risk are those less likely to be threats to national security. The border exception has been used to single out "[i]nnocent people from all walks of life . . . [including] lawyers and journalists."[185] Especially as these individuals work with or report on migrants on both sides of the border, they are uniquely reliant on storing confidential data on electronic devices they travel with internationally.

Second, the Court could increase the level of suspicion required to extract data in a forensic electronic device border search to probable cause. This might meaningfully reduce CBP's practice of performing forensic electronic device searches. If the practice was sufficiently diminished, then cartels would feel less need to change their behavior in a way that would modestly diminish the efficiency of their smuggling. Then, when CBP has probable cause for a particular traveler, that

---

[185] Sophia Cope, *Protecting Digital Data at the U.S. Border*, AM. CONST. SOC'Y (Sep. 11, 2019), https://www.acslaw.org/issue_brief/briefs-landing/protecting-digital-data-at-the-u-s-border/#_ftn17 [https://perma.cc/7T6F-JUVH] (collecting examples); Tom Jones, et. al., S*ource: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database*, NBC7 SAN DIEGO (Mar. 6, 2019), https://www.nbcsandiego.com/news/local/source-leaked-documents-show-the-us-government-tracking-journalists-and-advocates-through-a-secret-database/3438/ [https://perma.cc/V6F3-P4KG].

traveler is more likely to have inculpating information on their device that will be useful to targeting other smugglers or collaborators.

However, there are several flaws this this solution. First, requiring probable cause for a border search might seriously gut CBPs ability to prevent dangerous contraband. It is unrealistic that border "law enforcement is expected to ascertain individualized suspicion" when thousands of travelers cross the U.S. border each day.[186] Such burdens are weighty on the government. Furthermore, it is highly unlikely that current Fourth Amendment doctrine supports such a view. No court has ever applied more than reasonable suspicion at the border. A use-restriction regime firstly allows CBP to quickly extract data from any traveler while still retaining fidelity to the border search doctrine and protecting individual privacy.

VI. CONCLUSION

The border exception to the Fourth Amendment is a gross intrusion into the privacy expectations of travelers. It is unfair that routine inspections that travelers have become accustomed to have snowballed into full on invasions of their personal lives through suspicionless forensic electronic device searches.

The circuit splits regarding the purpose of the border exception traverse the spectrum. However, applying use restrictions by separating different uses of data as separate searches ameliorates discrepancies between courts and more importantly protects the privacy of travelers. Adopting such an analysis for border search exception searches would also protect the precedent of *Riley*, without derailing border enforcers' abilities to prevent contraband from entering and to prevent large-scale transnational crimes.

Applying such an analysis has strong doctrinal underpinnings in the border context. Because the searches are reasonable only within the scope of the exception's purpose, it would not make sense for law enforcement to be able to use seized data for a different purpose without a separate reasonableness assessment. Although the Supreme Court has not formally approved use-restrictions, adopting them in this context aligns neatly with previous lower court applications and fits situations where the Supreme Court has signaled a willingness to adopt such restrictions.

Consequences of over-collection of data could be dire. With regular database hacking, dubious lack of oversight for regular CBP personnel, and historic misuse by database managers, travelers' personal information like private photos, messages, and recordings are at risk of

---

[186] Kolsuz, 890 F.3d at 150 (Wilkinson, J., concurring).

being released to the public. And while law enforcement retaining individuals' information indefinitely is concerning enough, worse yet is the data being released to the world.