NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ELECTRONIC BORDER SEARCHES AFTER *RILEY*

by

Aaron Bode

December 2020

Co-Advisors: David W. Brannan (contractor)
Carolyn C. Halladay

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
ELECTRONIC BORDER SEARCHES AFTER *RILEY*

5. FUNDING NUMBERS

6. AUTHOR(S) Aaron Bode

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This thesis discusses the implications of the Supreme Court's 2014 decision in *Riley* v. California for the search of electronic devices at the border, termed "electronic border searches." It explores the degree to which such searches continue to be constitutionally permissible and contrasts *Riley's* categorical rule protecting electronic devices in the interior with the general search power granted the government at the border. Following an examination of the divergences among lower courts in applying *Riley*, it finds *Riley* has limited application to the conduct of electronic border searches and that they continue to be constitutionally permissible. This thesis also explores how the reasonableness of such searches can be maintained despite evolving technology and privacy perceptions. By examining other legislative and constitutional rules, it derives an approach for electronic border searches where powerful government interests and privacy concerns collide. The result is a view of electronic devices at the border as hybrid property—as both containers and novel "effects." Accordingly, this thesis advocates a hybrid-scope-limited approach that tethers suspicion-less electronic border searches to the original rationale for the border search doctrine. It presents a bifurcated framework leading to a two-tiered, hybrid-scope-limited rule where distinct levels of intrusion into electronic devices at the border are tied to differential levels of suspicion.

14. SUBJECT TERMS electronic, border search, electronic border search, Fourth Amendment, reasonableness	**15. NUMBER OF PAGES** 113
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

ELECTRONIC BORDER SEARCHES AFTER *RILEY*

Aaron Bode
Special Agent, Immigration and Customs Enforcement,
Homeland Security Investigations, Department of Homeland Security
BA, University of Florida, 1998
JD, University of Wisconsin, 2000

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2020**

Approved by: David W. Brannan
Co-Advisor

Carolyn C. Halladay
Co-Advisor

Erik J. Dahl
Associate Professor,
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis discusses the implications of the Supreme Court's 2014 decision in *Riley v. California* for the search of electronic devices at the border, termed "electronic border searches." It explores the degree to which such searches continue to be constitutionally permissible and contrasts *Riley's* categorical rule protecting electronic devices in the interior with the general search power granted the government at the border. Following an examination of the divergences among lower courts in applying *Riley*, it finds *Riley* has limited application to the conduct of electronic border searches and that they continue to be constitutionally permissible. This thesis also explores how the reasonableness of such searches can be maintained despite evolving technology and privacy perceptions. By examining other legislative and constitutional rules, it derives an approach for electronic border searches where powerful government interests and privacy concerns collide. The result is a view of electronic devices at the border as hybrid property—as both containers and novel "effects." Accordingly, this thesis advocates a hybrid-scope-limited approach that tethers suspicion-less electronic border searches to the original rationale for the border search doctrine. It presents a bifurcated framework leading to a two-tiered, hybrid-scope-limited rule where distinct levels of intrusion into electronic devices at the border are tied to differential levels of suspicion.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The border search doctrine authorizes U.S. customs officers to conduct warrantless, suspicion-less searches of persons and property crossing the U.S. border.[1] Since the Supreme Court's 2014 decision in *Riley v. California*, arguments that electronic devices and their accompanying data qualify as a different type of property that should be protected from general searches at the border have grown.[2] This thesis examines whether, in the aftermath of *Riley*'s declaration of special categorical protection for electronic devices in the interior, general searches of electronic devices at the border are Constitutional. An analysis of decisions by lower courts that confronted the electronic border search question since *Riley* finds that some reject equating electronic devices to other physical containers crossing the border and that such searches are only reasonable "if relevant government interests are present."[3] Other courts have gone further and significantly narrowed customs officers' authority to conduct electronic border searches.[4] Still others, however, have, in light of the historic breadth of the government's authority to search people and property at the Nation's borders, found *Riley* irrelevant.[5] The result is significant divergence in opinion within the U.S. judiciary as to the reasonableness of the government's conduct of electronic border searches, including their proper scope and manner. In answering this question, this thesis finds that unique aspects of the *Riley* decision itself, its context, and circumstances demand a narrow, vice broad, application of its holding. Furthermore, this thesis explains that given their provenance and abundant statutory support, border searches, including those of electronic devices and data, are an *exemption* to the Fourth Amendment, not an

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

[2] Laura K. Donohue, "Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches," *Yale Law Journal Forum* 128 (2019): 961–1015, https://www.yalelawjournal.org/forum/customs-immigration-and-rights; Thomas Mann Miller, "Digital Border Searches after *Riley v. California*," *Washington Law Review* 90, no. 4 (2015): 1943–96.

[3] United States v. Kolsuz, 890 F.3d 133, 142, 145–46 (4th Cir. 2018).

[4] United States v. Cano, 934 F.3d 1002 (9th Cir. 2019); Alasaad v. McAleenan, No. 17-cv-11730-DJC (D. Mass. Nov. 12, 2019).

[5] United States v. Vergara, 884 F.3d 1309 (11th Cir. 2018); United States v. Touset, 890 F.3d 1227 (11th Cir. 2018).

exception like the searches at issue in *Riley*. As a result, despite the fervor created by *Riley*, electronic border searches continue to be a Constitutionally reasonable exercise of the broad authority vested in customs officers over all that enters and exits the country.

This thesis also addresses a second question: how can the reasonableness of electronic border searches be maintained in the face of evolving technology and concomitant privacy concerns that troubled the *Riley* Court? To answer this question, a view of electronic devices and their stored data as a hybrid form of property is presented. This perspective recognizes the duality of electronic devices—as both containers and novel effects—where powerful government and individual privacy interests collide. In discussing this perspective, this thesis details other constitutionally sanctioned approaches that balances these competing interests when new technology and new threats emerge. In addition to an examination of the border search doctrine itself and a discussion as to how electronic devices should be treated under the doctrine moving forward, this thesis reviews other existing U.S. statutory regimes specifically developed for governing government access to information in which people have significant privacy expectations. The resulting deductive and inductive analysis details how the hybrid view empowers the government to counter novel threats at the border while protecting privacy in data that does not pertain to the government's broad rationale for conducting suspicion-less border searches. In presenting the hybrid model for electronic devices at the border, its advantages, including its maintenance of technological and mode neutrality in border searches of all property as well its ability to adapt to changing privacy attitudes, are discussed.[6]

Building on this hybrid view of electronic devices at the border, this thesis outlines a hybrid-scope-limited approach for electronic border searches. This approach tethers suspicion-less electronic border searches to the original rationale underlying the border search doctrine which encompass the following areas:

[6] See Orin S. Kerr, "Applying the Fourth Amendment to the Internet: A General Approach," *Stanford Law Review* 62, no. 4 (2010): 1005–49; Richard McAdams, "*Riley*'s Less Obvious Tradeoff: Forgoing Scope-Limited Searches," *Texas Tech Law Review* 48 (2015): 97–131; Thomas K. Clancy, "Fourth Amendment Satisfaction—The 'Reasonableness' of Digital Searches," *Texas Tech Law Review* 48 (2015): 37–63; and *Ramsey*, 431 U.S. 606.

- national security,
- the collection of duty and regulation of trade,
- preventing the introduction of harmful goods, and
- regulating immigration to prevent the entry of illegal, inadmissible, or unwanted persons.

A two-tiered framework for the implementation of this approach is then introduced in which distinct levels of government intrusion into electronic devices at the border are tied to differential levels of suspicion. Within this discussion, this thesis examines the reasonableness of such searches using forensic tools that allow for a search of all data present on an electronic device, including that which has been deleted and that which is opaque to the user. In addition, it presents an analysis as to why reasonable suspicion, following the accepted definition of that term from the Supreme Court's decision in the *Terry v. Ohio*, should be the standard for electronic border searches of increased scope and manner—so-called second-tier searches.[7] Ultimately, this thesis advances a tiered, hybrid-scope-limited rule that adheres to the long-established border dynamic where the government's authority is at its "zenith" and an individual's right to privacy is greatly diminished.[8] This construct provides guidance to customs officers for dealing with the unique issues involved in conducting electronic border searches. In doing so, it allows for the maintenance of reasonableness, now and in the future, in the depth, breadth, and manner of customs officers' intrusions into digital property at the border.

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

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

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisors, Dr. Carolyn Halladay and Dr. David Brannan, for their guidance in the creation and completion of this work. I owe a special thank you to Marianne Taflinger who graciously reviewed every part of this thesis, was very supportive, and who greatly improved the piece's clarity. I, however, am most indebted to my girls at home. As always, throughout this process they have been most patient, most loving, and most kind.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THE BORDER SEARCH DOCTRINE AND ELECTRONIC DEVICES

The border search doctrine, as it exists in the United States, holds that all persons and property, when crossing the nation's borders, are subject to suspicion-less search. The purpose is simply to protect the nation and the people from a host of threats. For this reason, customs offices can search anything that crosses the border, whether it be a suitcase, a parcel, a shipping container, or a person, without warrant or probable cause. And aside from invasive searches of a person's body, no justification for the search is necessary. However, with the advent of modern electronic devices—and in light of the extensiveness of their use and the nature of the data they contain—the question arises as to whether these devices should receive the same treatment under the border search doctrine as any other suitcase or container.

Are electronic devices somehow different for the purposes of search by law enforcement officials? In 2014, the Supreme Court issued a decision in *Riley v. California* which for the first time accorded electronic devices increased protection from government searches—in this case, search incident to arrest of a person inside the United States—beyond that of traditional property.[1] Since then, the momentum of *Riley* has inspired some courts to extend this logic to other kinds of searches—right up to the U.S. borders. Based on a careful analysis of the relevant law and practice—beginning with the unique character of the border search doctrine itself—this thesis argues that despite the *Riley* decision, searches of electronic devices at the border, do not violate the Constitution. This thesis, however, goes further and recognizes that the technological innovations of the future represent an unending challenge to the government's border authority over electronic devices and the digital property they hold. Consequently, this thesis argues that searches of electronic devices need a structure to ensure their scope and the manner in which they are conducted maintain their reasonableness in the future. This thesis proposes such a

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

structure with a tiered, hybrid-scope-limited conceptual framework that will make electronic border searches effective and secure their continued constitutionality.

A. PROBLEM STATEMENT

The border search doctrine allows certain government officials to conduct warrantless, suspicion-less searches of persons and property crossing the U.S. border.[2] Despite Fourth Amendment requirements that typically prohibit general searches—"fishing expeditions" in modern parlance—searches at the border, particularly routine searches, have long been viewed as different.[3] Unlike inside the country, where the protection of personal liberty is the pre-eminent concern, at the border, the government's interest in protecting the nation and the people from harm through robust search powers reigns supreme.

In light of the *Riley* decision, the U.S. circuit courts disagree as to whether electronic border searches should be permissible under the Fourth Amendment or constitute unreasonable infringements of individuals' privacy.[4] Neither Congress nor the Supreme Court has taken definitive action or given clear direction in this regard, leaving executive agencies uncertain about how to establish a proper practice. In some areas of the country, notably in the Ninth Circuit, electronic border searches have been all but prohibited except for a narrow exception.[5] Others, like the Eleventh Circuit, however, have upheld the practice as entirely constitutional despite *Riley*.[6] Some circuits, like the Fourth Circuit, have attempted to reconcile *Riley* with existing border search precedent.[7] Still other circuits, among them the Seventh and Tenth Circuits, in failing to delineate clear

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

[3] United States v. Montoya de Hernandez, 473 U.S. 531, 537–541 (1985).

[4] Gina Bohannon, "Cell Phones and the Border Search Exception: Circuits Split over the Line between Sovereignty and Privacy," *Maryland Law Review* 78, no. 3 (2019): 563–603.

[5] United States v. Cano, 934 F.3d 1002 (9th Cir. 2019).

[6] United States v. Touset, 890 F.3d 1227 (11th Cir. 2018).

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

reasonableness standards, have demonstrated their own indecision and apprehension in the face of these electronic border search questions.[8]

Amid the current legal upheaval, however, customs officers have been left in an increasingly untenable position.[9] They are charged with wielding broad authority without clear legal guidance in how to properly circumscribe electronic border searches.[10] In addition, open questions surround government detention of electronic devices as well as which steps customs officers may take in overcoming device passwords and encryption when exercising their border authority.[11] The lack of legal clarity has ultimately left the government vulnerable to losing items of evidence that could be used in support of prosecutions that increase national security and uphold the nation's customs and immigration laws.[12] These vagaries have also exposed the government and homeland security practitioners as individuals to civil liability for actions taken in an increasingly gray area at the nation's borders.[13]

B. RESEARCH QUESTIONS

1. In light of the Supreme Court's decision in *Riley v. California*, should warrantless electronic border searches continue to be constitutionally permissible?

2. If so, how can customs agents execute electronic border searches, in manner and scope, to ensure continuing reasonableness?

---

[8] See, for example, United States v. Wanjiku, 919 F.3d 472 (7th Cir. 2019); and United States v. Williams, 942 F.3d 1187 (10th Cir. 2019).

[9] Hillel R. Smith, *Do Warrantless Searches of Electronic Devices at the Border Violate the Fourth Amendment?*, CRS Report No. LSB10387 (Washington, DC: Congressional Research Service, 2019).

[10] Smith.

[11] Laura Nowell, "Privacy at the Border: Applying the Border Search Exception to Digital Searches at the United States Border," *Federal Communications Law Journal* 71, no. 1 (2019): 85–104.

[12] *Cano*, 934 F.3d 1002.

[13] Alasaad v. McAleenan, No. 17-cv-11730-DJC (D. Mass. Nov. 12, 2019). For example, if a customs officer conducts an electronic border search of a traveler's devices pursuant to the government's historically recognized broad border authorities and a court deems that search unconstitutional, reasoning *Riley* demands that electronic devices receive special protection, that customs officer could be subject to a *Bivins* action for violating the traveler's constitutional rights.

C. LITERATURE REVIEW

Reasonableness under the Fourth Amendment is a nebulous concept that can vary depending on the facts of a given case. Also, what is considered reasonable depends on the object of the search or seizure. Proper conduct in searching a vehicle can be unreasonable when searching a home. Which type of government activity is constitutionally sanctioned differs whether the search of a property or a person. Consequently, to determine whether a border search of electronic devices and data is constitutionally reasonable post-*Riley*, one must first ascertain the category of property into which modern electronic devices fall. An answer here determines the degree of legal protection afforded these devices. To date, however, no universal legal construct definitively categorizing electronic devices and defining their treatment as property has emerged.

Leading Fourth Amendment legal scholars have struggled with how to approach electronic device searches as a subcategory of property searches.[14] Despite being intangible, data stored on these devices is property. And much of this data has physical world analogues for which established Fourth Amendment rules exist. Data, however, can be highly personal. Thus, concerns about dignity and privacy intrusions resulting from searches of electronic devices carry greater weight than in other property searches.[15] The hybrid nature of electronic devices and data—paralleling traditional property in some aspects but being completely novel in others—has strained traditional Fourth Amendment

[14] Orin S. Kerr, "Fourth Amendment Seizures of Computer Data," *Yale Law Journal* 119, no. 4 (2010): 700–724.

[15] See, for example, United States v. Ickes, 393 F.3d 501 (4th Cir. 2005); Constitution Project, *Suspicionless Laptop Searches under the Border Search Doctrine: Legal and Privacy Concerns with the Department of Homeland Security's Policy* (Washington, DC: Constitution Project, 2011); Christine A. Coletta, "Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment," *Boston College Law Review* 48, no. 4 (2007): 971–1007; Victoria Wilson, "Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States Borders from Bombs, Drugs, and the Pictures from Your Vacation," *University of Miami Law Review* 65, no. 3 (2011): 999–1025; Scott J. Upright, "Suspicionless Border Seizures of Electronic Files: The Overextension of the Border Search Exception to the Fourth Amendment," *William and Mary Law Review* 51, no. 1 (2009): 291–326; Ari B. Fontecchio, "Suspicionless Laptop Searches under the Border Search Doctrine: The Fourth Amendment Exception That Swallows Your Laptop," *Cardozo Law Review* 31 (2009): 231–66; Laura K. Donohue, "Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches," *Yale Law Journal Forum* 128 (2019): 961–1015, https://www.yalelawjournal.org/forum/customs-immigration-and-rights; and Thomas Mann Miller, "Digital Border Searches after *Riley v. California*," *Washington Law Review* 90, no. 4 (2015): 1943–96.

rules, which, like the border search doctrine, bifurcate searches into general categories of property and people.[16] At the border, this distinction is stark; searches of property do not carry the same compelling personal dignity concerns that invasive searches of the body do.[17]

Significant heterogeneity in how electronic devices, as new technology, should be treated within the general category of property under the Fourth Amendment has developed.[18] Divergent views have been articulated in the context of Fourth Amendment searches generally and in the context of border searches specifically.[19] Some courts and observers have considered electronic devices as a type of personal container holding data much as other containers, like filing cabinets, hold a person's papers.[20] Rules governing containers in the context of the Fourth Amendment have been well-delineated.[21] Several courts considering border searches of laptop computers have followed the container theory in refusing to carve out special protections for such devices.[22] These courts have equated

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

[17] *Flores-Montano*, 541 U.S. 149.

[18] See, for example, Thomas K. Clancy, "Fourth Amendment Satisfaction—The "Reasonableness" of Digital Searches," *Texas Tech Law* Review 48 (2015): 37–63; Orin S. Kerr, "An Equilibrium-Adjustment Theory of The Fourth Amendment," *Harvard Law Review* 125, no. 2 (2011): 476–543; Orin S. Kerr, "Foreword: Accounting for Technological Change," *Harvard Journal of Law and Public Policy* 36, no. 2 (Spring 2013): 403–8; Orin S. Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," *Michigan Law Review* 102, no. 5 (March 2004): 801, https://doi.org/10.2307/4141982; Cynthia Lee, "Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us about the Fourth Amendment," *Journal of Criminal Law & Criminology* 100, no. 4 (Fall 2010): 1403–94; Richard McAdams, "*Riley*'s Less Obvious Tradeoff: Forgoing Scope-Limited Searches," *Texas Tech Law Review* 48 (2015): 97–131; and Christopher Slobogin, "An Original Take on Originalism," *Harvard Law Review* 125, no. 2 (2011): 14–22.

[19] See, for example, Patrick Corbett, "The Future of Digital Evidence Searches and Seizures: The Future of the Fourth Amendment in a Digital Evidence Context: Where Would the Supreme Court Draw the Electronic Line at the International Border?," *Mississippi Law Journal* 81, no. 5 (2012): 1263–1308; Sid Nadkarni, "'Let's Have a Look Shall We?' A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices," *UCLA Law Review* 61 (2013): 146–94; Nathan A. Sales, "Run for the Border: Laptop Searches and the Fourth Amendment," *University of Richmond Law Review* 43, no. 3 (2009): 1091–1134; and Rachel Flipse, "An Unbalanced Standard: Search and Seizure of Electronic Data under the Border Search Doctrine," *University of Pennsylvania Journal of Constitutional Law* 12, no. 3 (2010): 851–74.

[20] Orin S. Kerr, "Searches and Seizures in a Digital World," *Harvard Law Review* 119, no. 2 (2005): 539.

[21] Kerr, 550.

[22] United States v. Arnold, 33 F.3d 1003 (9th Cir. 2008).

laptop computers with physical pieces of luggage containing personal property subject to suspicion-less border searches.[23] This so-called container view of electronic devices has been further reflected in the border search policies of Customs and Border Protection and Immigration and Customs Enforcement—Homeland Security Investigations.[24] Other courts have even used the container analogy to reason that, at the border, electronic devices and their data are simply cargo.[25] Proponents of this perspective laud the container theory for its technological neutrality.[26] Treating electronic devices as personal containers allows for the application of traditional rules regarding reasonableness, which at the border means all data contained within is subject to full examination without suspicion or a warrant.

The container theory, however, has not garnered consensus. Many reject treating electronic devices as containers and data as personal chattel. Several articles have questioned whether it is logical, given the potential privacy implications, to treat a laptop and its stored data as only another piece of luggage.[27] Critics argue that electronic devices carry data previously only contained in private homes.[28] Moreover, these devices can carry this private information in quantities previously unimaginable.[29] Critics reason that but for these devices, people would not be carrying this type and quantity of private information across international boundaries.[30] In other words, electronic devices differ significantly

[23] *Arnold*, 33 F.3d at 1007.

[24] Customs and Border Protection, *Border Searches of Electronic Devices*, Directive No. 3340-049A (Washington, DC: Customs and Border Protection, 2018); Immigration and Customs Enforcement, *Border Searches of Electronic Devices*, Directive No. 7-6.1 (Washington, DC: Immigration and Customs Enforcement, 2009).

[25] *Ickes*, 393 F.3d 501.

[26] Sales, "Run for the Border," 1114–15.

[27] Kevin Fayle, "Dignity, Privacy and Hard Drives: Laptops and the Border Search Exception to the Fourth Amendment," *Law/Technology* 41, no. 4 (2008): 24; Wilson, "Laptops and the Border Search Exception to the Fourth Amendment," 1009; Fontecchio, "Suspicionless Laptop Searches," 249–53.

[28] Sunil Bector, "Your Laptop, Please: The Search and Seizure of Electronic Devices at the United States Border," *Berkeley Technology Law Journal* 24, no. 1 (2009): 705.

[29] Rasha Alzahabi, "Should You Leave Your Laptop at Home When Traveling Abroad? The Fourth Amendment and Border Searches of Laptop Computers," *Indiana Law Review* 41, no. 1 (2008): 178–83, https://doi.org/10.18060/3928. Nathan Sales points out that a 250 GB hard drive can store "the equivalent of 125 million printed pages of text" and that "only sixty-three" 250 GB hard drives would be needed to "store the entire collection of the Library of Congress." Sales, "Run for the Border," 1099–1100.

[30] Alzahabi, "Should You Leave Your Laptop at Home?," 179.

from baggage carrying a traveler's personal items. As a result, many scholars express concern that placing these devices under the universal merchandise umbrella, without special designation, affords border agents the ability to intrude on personal privacy on a frightening scale without justification.[31]

In particular, container-theory contrarians argue a special approach to electronic devices at the border needs to be adopted.[32] Under this approach, observers postulate the government should be required to obtain at least some level of suspicion of criminal activity for electronic border searches to be constitutionally reasonable.[33] Some in Congress have adopted this view, arguing electronic devices deserve increased protection at the border.[34]

Some courts have begun to rethink the container view. For example, courts have recognized that a border search using forensic software will recover information on the device that the user has deleted and may be unaware of its continued presence.[35] Thus, if an electronic device is no different from a suitcase, a forensic search of the device is akin to not only searching the contents of the suitcase currently stored therein but also anything that has ever been carried in that suitcase.[36] Still other courts continue to apply traditional property rules to electronic devices at the border. Specifically, these courts note, among other things, that electronic devices can contain material electronically that carried in a physical form across the border would be unquestionably subject to search regardless of how private the material.[37] They question the logic of granting special protections for property crossing the border based simply on the form in which it is carried.[38]

---

[31] Eunice Park, "The Elephant in the Room: What Is a 'Nonroutine' Border Search, Anyway? Digital Device Searches Post-*Riley*," *Hastings Constitutional Law Quarterly* 44 (2017): 298–300.

[32] Clancy, "Fourth Amendment Satisfaction," 38.

[33] Constitution Project, *Suspicionless Border Searches of Electronic Devices*, 11.

[34] Fayle, "Dignity, Privacy and Hard Drives," 24.

[35] United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013).

[36] *Cotterman*, at 965.

[37] *Touset*, 890 F.3d 1227.

[38] *Touset*, at 1236.

Advocates of treating electronic devices and their data as a special category of property at the border, however, have failed to reach consensus on the degree of special protection required. Some have articulated the government should have probable cause and possibly a warrant for border searches of electronic devices where files are to be copied as they are in forensic border exams.[39] Others have argued for the need for reasonable suspicion.[40] Still others consider electronic devices as a type of property in which the government may intrude without warrant so long as customs officers have at least one reason for doing so.[41] These varying ideas about the level of justification customs agents need to penetrate the sanctity of individuals' electronic devices creates uncertainty about the extent border authorities can be exercised vis-à-vis such property.

The evolution of electronic devices and the Supreme Court decision in *Riley* have further confused rather than clarified the question of how electronic devices should be considered at the border. The debate has grown from arguments over whether these devices require a special approach to arguments declaring them to be novel forms of property under the Fourth Amendment. Those presenting the latter position claim that searches of personal electronic devices are more than property searches equivalent to searches of a person's "brain."[42] As such, these observers argue, the border search of electronic devices require new rules. In Congress, Senators sponsoring the Protecting Data at the Border Act in 2018 argued that electronic devices should receive dissimilar treatment under law.[43] Such novel treatment could result in electronic devices and their data protected at the border to the same or greater degree than a person's body. This extremity carries the potential to nullify any application of the border search doctrine to electronic devices regardless of the weight of government interests involved.

---

[39] Upright, "Suspicionless Border Seizures of Electronic Files," 323–24.

[40] Kelly A. Gilmore, "Preserving the Border Search Doctrine in a Digital World: Reproducing Electronic Evidence at the Border," *Brooklyn Law Review*, 72, no. 2 (2007): 792.

[41] Fontecchio, "Suspicionless Laptop Searches," 266.

[42] Coletta, "Laptop Searches at the United States Borders," 1007.

[43] *Examining Warrantless Smartphone Searches at the Border: Hearing before the Subcommittee on Federal Spending Oversight and Emergency Management of the Committee on Homeland Security and Governmental Affairs*, Senate, 115th Cong., 2nd sess., July 11, 2018, 2.

Further confounding efforts to develop a coherent approach to electronic devices at the border has been the rapid development and societal adoption of smartphones. To many, smartphones represent rich repositories of the most intimate details of life—and also a necessity in today's world.[44] Thus, recent critics of suspicion-less electronic border searches have argued that smartphones stand apart from traditional forms of property and all other electronic devices.[45] Some in Congress have noted with incredulity attempts to equate smartphones with suitcases.[46] Hence, electronic border search critics believe that both the volume of intimate information smartphones contain and its quality justifies the novel property categorization of these devices.[47] In other words, a person cannot put in a suitcase as much self-revealing material as he or she puts on a smartphone—intentionally or nor. For example, a smartphone contains data on a user's movements and locations as well as applications that track everything from the user's health symptoms to religious and political affiliations.[48] Thus, questions of special designations and protections of personal smartphones, independent of all other electronic devices, have fueled the growing electronic border search dilemma.

The current state of conflicting case law involving electronic border searches reveals the judiciary's struggle in considering electronic devices as property.[49] As courts continue to review electronic border searches, with increasing focus on searches of personal smartphones, consensus appears ever more remote. Some have questioned whether courts should be taking the lead in determining whether new types of technology receive disparate levels of Fourth Amendment protection.[50] In fact, given the nature of the judicial process, courts are ill-positioned to make such decisions.[51] Some scholars have even used the *Riley* decision and the rationale of the Court in that case to illustrate, that

[44] *Riley*, 573 U.S. at 2485–86, 2493–98.

[45] Donohue, "Customs, Immigration, and Rights," 999, 1002–3.

[46] S., *Examining Warrantless Smartphone Searches at the Border*, 2.

[47] Donohue, "Customs, Immigration, and Rights," 1006.

[48] Miller, "Digital Border Searches after *Riley*," 1978.

[49] "The Border Search Muddle," *Harvard Law Review* 132 (2019): 2279.

[50] Mary Leary, "The Supreme Digital Divide," *Texas Tech Law Review* 48 (2015): 70–72.

[51] Leary, 92–94.

courts have a poor understanding of evolving technology in the context of modern life.[52] Thus, the resulting Fourth Amendment rules become unsustainable in the long term because rather than striking a balance between government interests and individual liberty, the Court's rationale leads to reactionary, ad hoc decisions incapable of adaptation.[53]

Learned observers make compelling arguments that courts, traditionally the arbiters of Fourth Amendment reasonableness, should exercise caution when considering new technologies and novel treatment.[54] Instead of declaring electronic devices and data to be akin to other forms of property or forging new categories with new rules, they call for courts to exercise restraint and use legislative trends as guides.[55] To these scholars, the question as to which type of property electronic devices are to be considered under the Fourth Amendment, and as such, any added degrees of protection they may have, is one of societal considerations of reasonableness.[56] Specifically, properly categorizing electronic devices and their data as property depends on how private the American body politic finds them; and what additional requirements, if any, should be imposed on the government prior to conducting electronic searches, regardless of search location.[57] Therefore, many observers argue that Congress could better answer how electronic devices should be treated under the Fourth Amendment: in short, are electronic devices like traditional containers, a special type of property requiring modification to traditional rules, or a novel category of property requiring greater protection than other types of personal chattel.[58] As courts have tackled this question in the context of border searches, stark contrasts in definitions of reasonableness and conflicting rulings have emerged.[59]

---

[52] Leary, 72–90.

[53] Leary, 85.

[54] Kerr, "The Fourth Amendment and New Technologies," 801.

[55] Kerr, 875–77.

[56] Leary, "The Supreme Digital Divide," 92.

[57] Kerr, "The Fourth Amendment and New Technologies," 884–88.

[58] Kerr, 855–60.

[59] See, for example, *Kolsuz*, 890 F.3d 133; *Touset*, 890 F.3d 1227; *Cano*, 934 F.3d 1002; and *Alasaad*, No. 17-cv-11730-DJC.

D. THE BORDER SEARCH DOCTRINE: STATUTES AND CASE LAW

Until the arrival of *Riley*, border search law had marked stability and there was significant statutory and precedential deference. The border search doctrine, which de-emphasizes personal rights in favor of territorial sovereignty, was codified by the First Congress on July 31, 1789, and predates the passage of the statutes that would come to be known as the Bill of Rights.[60] In sections 23–26 of an act titled "the Collection of the Duties Imposed by law on the Tonnage of Ships or Vessels, and on Goods, Wares and Merchandises Imported into the United States," Congress authorized customs collectors and other officers to enter any ship or vessel and search wherever for any goods, wares, or merchandise that may be found.[61] In 1790, Congress further authorized customs officers to "free[ly] access" anything entering the country including "any box, trunk, chest, cask, or other package."[62] Modern border search statutes, rooted in these early acts, have continued to provide for "plenary" customs officer search authority.[63] For example, Title 19 U.S.C. § 1581(a) specifically allows customs officers to, among other things, examine, inspect, and search "any person, trunk, package, or cargo."[64] By the same token, Title 19 U.S.C. § 482, authorizes customs officers, in part, to "stop, search, and examine . . . any person" and to search any property transiting the border including all manner of personal goods, even "envelope[s]."[65] At the border, all property is considered "merchandise."[66] "Merchandise" itself is defined, per the Tariff Act of 1930, as "goods, wares, and chattels of every description . . . includ[ing] merchandise the importation of which is prohibited."[67] Per the statute, "merchandise" is not confined to commerce but applies to individuals' personal

---

[60] Richard Peters, ed., *The Public Statutes at Large of the United States of America, from the Organization of the Government in 1789, to March 3, 1845*, vol. 1 (Boston: Charles C. Little and James Brown, 1845), 29–49, https://www.loc.gov/law/help/statutes-at-large/1st-congress/c1.pdf.

[61] Peters, 43.

[62] Peters, 164.

[63] *Ramsey*, 431 U.S. at 616.

[64] 19 U.S.C. § 1581(a) (2010). See also 19 U.S.C. § 1461 (2011); 19 U.S.C. § 1582 (2008); and 19 C.F.R. §§ 162.6–162.7 (2012).

[65] 19 U.S.C. § 482 (2010). See also 19 U.S.C. § 1467 (2011), which further authorizes customs officers to search "persons, baggage, or merchandise" arriving from foreign locales.

[66] 19 U.S.C. § 482.

[67] 19 U.S.C. § 1401(c) (2011).

property as well.[68] In short, Congress has stated that every*thing* is subject to search at the border.

Other statutes further delineate border search authority and reinforce its intended broad scope. Title 19 U.S.C. § 1461 authorizes the border inspection of "merchandise and baggage" and requires a person carrying "any trunk, traveling bag, sack, valise, or other container, or of any closed vehicle, to open the same for inspection, to furnish a key or other means for opening same."[69] Title 19 U.S.C. § 1467 authorize searches of "persons, baggage, or merchandise," to ensure compliance with all customs "laws, regulations, and instructions" as well as those that the "Customs Service" enforces.[70] Title 19 U.S.C. § 1582 authorizes the search of persons and baggage entering the United States in accordance with additional regulations.[71] These include Title 19 Code of Federal Regulations (C.F.R.) Part 162.6, which authorizes the border search of "all persons, baggage, and merchandise," arriving in the United States from a foreign country or territory.[72] Another, Title 19 C.F.R. Part 162.7 authorizes the "stop, search, and examin[ation] [of] any vehicle, person, or beast, or search [of] any trunk or envelope *wherever* found" (emphasis added).[73] Well before *Riley*, Congress even confirmed that the broad customs authority over all property crossing the border included electronic devices and data. Title 6 U.S.C. Sec 211(k)(A), still in effect, explicitly commands the Customs and Border Protection (CBP) commissioner to develop "standard operating procedures for searching, reviewing, retaining, and sharing

[68] Alfonso Robles, *Law Course for Customs and Border Protection Officers*, 13th ed. (Glynco, GA: Gould Publications, 2004), 159. Arriving individuals to the United States from places foreign are also subject to inspection and examination pursuant to 8 U.S.C. § 1357(c) (2011). This section and its statutory siblings specifically allow for the border search of individuals and their property for purposes of determining their admissibility. Though an important authority in the realm of border search, especially considering the government's authority to encounter foreign nationals and search their belongings, it is not as broad as the customs statutes discussed, as border searches under this heading are limited to the purposes of determining the person's admissibility. Consequently, we will focus on the broader customs statutes providing for the search of all things, i.e., merchandise, crossing the U.S. territorial boundaries.

[69] 19 U.S.C. § 1461.

[70] 19 U.S.C. § 1467.

[71] 19 U.S.C. § 1582.

[72] 19 C.F.R. § 162.6.

[73] 19 C.F.R. § 162.7.

information contained in *communication, electronic or digital devices encountered . . . at United States ports of entry*" (emphasis added).[74]

Based on this long statutory lineage, courts have routinely endorsed searches at the border as reasonable, do not require probable cause, and never require a warrant.[75] In 1886, the Supreme Court, in *Boyd v. United States*, conspicuously recognized the scope of the border search doctrine and its attendant statutes to be in complete harmony with constitutional protections.[76] Nearly 100 years later, in *U.S. v. Ramsey*, the Supreme Court, affirmed the "plenary power" given to customs officers to conduct searches at the border.[77] In declaring border searches "grounded in the recognized right of the sovereign to control . . . who and what may enter the country" the Court found "manifest" the "historical importance of the enactment of this customs statute by the same Congress which proposed the Fourth Amendment."[78] In subsequent cases, the Court established the precedent of affording deferential treatment to border search statutes given their "impressive historical pedigree."[79] The Supreme Court has so firmly established the reasonableness of government searches at the border including body searches as necessary "to protect the Nation."[80] Even in the digital age, the Court established as "axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity" and, at the international border, both are at their "*zenith*" (emphasis added).[81] This precedent acknowledged the border as exempt from Fourth Amendment protections in stark contrast to the interior of the country where personal liberty commands the greatest force.

---

[74] 6 U.S.C. § 211(k)(1)(A) (2014).

[75] Judith B. Ittig, "The Rites of Passage: Border Searches and the Fourth Amendment," *Tennessee Law Review* 40 (1973): 329.

[76] Boyd v. United States, 116 U.S. 616, 623 (1886).

[77] *Ramsey*, 431 U.S. at 616.

[78] *Ramsey*, 431 U.S. at 616–17, 620.

[79] United States v. Villamonte-Marquez, 462 U.S. 579, 585 (1983).

[80] *Montoya de Hernandez*, 473 U.S. at 538–39.

[81] *Flores-Montano*, 541 U.S. at 152–53.

Before *Riley*, electronic border searches were almost universally deemed reasonable based on comparing electronic devices to containers that warehoused data much in the same way that other physical containers hold tangible items.[82] This rationale led one observer to summarize that early views by courts of electronic border searches took the form of "border search exceptionalism."[83] One appellate ruling, five years before *Riley*, affirmed that the border search doctrine rested on the United States' "inherent sovereign authority to protect its territorial integrity" and such authority entitled the government "to require that whoever seeks entry must establish the right . . . to bring into the country whatever he may carry."[84] Another pre-*Riley* decision defined the government's search authority at the border to be "sweeping" and electronic border searches as entirely consistent with the Constitution.[85] These decisions relied on the language of border search statutes and the use of "the embracive term 'cargo.'"[86] The broad definition of "cargo" as "goods transported by a vessel, airplane, or vehicle," helped to outline the acceptable objects of search.[87] Congress' assiduous use of the word "any" in its border search statutes, especially as a modifier regarding what can be searched, was highlighted.[88] Thus, before *Riley*, electronic devices were "cargo" subject to such searches.

Only one appellate court before *Riley* stood even slightly apart from the "border search exceptionalism" perspective.[89] In 2013, a year before the *Riley* decision, the Ninth Circuit Court of Appeals in *U.S. v. Cotterman* discussed an electronic border search that included a forensic search of a traveler's personal laptop computer.[90] The *Cotterman* court compared border searches using forensic tools to "an exhaustive exploratory search," akin

[82] Miller, "Digital Border Searches after *Riley*," 1961.

[83] "The Border Search Muddle," 2280–81.

[84] *Arnold*, 33 F.3d at 1006–7.

[85] *Ickes*, 393 F.3d at 503, 505.

[86] *Ickes*, at 504.

[87] *Ickes*, at 504

[88] *Ickes*, at 504.

[89] "The Border Search Muddle," 2281.

[90] *Cotterman*, 709 F.3d 952.

to a strip search, that is "more intrusive than [searches of] other forms of property."[91] *Cotterman* noted that forensic searches will recover deleted information and tantamount to searching a container not only for its current contents but also for all of its previous contents.[92] As a result, *Cotterman* counter-balanced border search exceptionalist arguments with data exceptionalist arguments and found suspicion-less forensic border searches to be unreasonable.[93] Such was the state of electronic border search law before *Riley*.

E. RESEARCH DESIGN

In light of the *Riley* decision, this project combines legal along with deductive and inductive analysis to address the issues of the constitutionality of electronic border searches and their reasonableness in practice. It begins by looking at the ramifications of *Riley*, arguments for the severe truncation of electronic border searches, and the conflicting rules from the lower courts concerning the practice, given the history of the border search doctrine and *Riley*'s discussion of electronic devices as unique property. The thesis explores the compatibility of electronic border searches with the Fourth Amendment by viewing electronic devices and their stored data as hybrid property necessitating a scope-limited search approach. In doing so, it will detail other constitutionally sanctioned hybrid and scope-limited approaches developed to balance new technology, new threats, and government interests. Inductive analysis here will also involve an examination of existing U.S. statutory regimes specifically developed for governing government access to electronic data and for countering novel threats at the border. This deductive and inductive legal analysis will likely result in recommending a scope-limited rule for electronic border search that seeks to balance the government interests versus privacy rights.

Analysis then turns to the constitutionality of electronic border search in practice. It focuses on applying a scope-limited rule and dealing with unique challenges involved in

[91] *Cotterman*, at 962–64, 966.

[92] *Cotterman*, at 965.

[93] "The Border Search Muddle," 2282. This source articulates the data-exceptionalist perspective in *Riley* and evident in subsequent electronic border search cases.

searches of electronic devices. This thesis also discusses tethering electronic border search protocols to existing legal regimes governing the search of novel technology including devices and data that have been accepted as constitutionally sound. This approach highlights the comparative reasonableness of electronic border searches conducted using these protocols. Ultimately, this thesis argues that a hybrid-scope-limited approach to electronic border searches is both permissible and desirable post-*Riley*, and it identifies protocols that should be enshrined in agencies' policies to guide practitioners in reasonable conduct.

This project focuses specifically on U.S. customs authorities governing searches under the border search doctrine. Consequently, it examines electronic border searches in the context of merchandise. The totality of the border search doctrine is also based on immigration inspection authorities like the those found in Title 8 U.S.C. § 1357(c). This legal authority could similarly be used to inform a scope-limited electronic border search approach. Because, however, these authorities do not apply universally but only to arriving persons of alienage, an analysis as to how this authority might shape the scope of electronic border searches lies beyond the bounds of this paper. This paper also does not distinguish between the different agencies, officers, and agents who possess border search authority nor the differences in specific duties of each. Rather, all are treated under the monolithic "customs officers" as defined in the U.S Code. Accordingly, this thesis will not explore any differences in duties and agency mission which might influence a scope-limited approach. Although the protocols analyzed and explained based on the hybrid-view/scope-limited approach could provide significant guidance, this work also will not directly address the sharing of data garnered during electronic border searches with other law enforcement or intelligence agencies.

F. OVERVIEW OF CHAPTERS

This thesis consists of five chapters. Chapter I has identified the problem confronting the current practice of electronic border searches since *Riley*. This chapter has set forth the research questions this thesis attempts to answer. It has reviewed the literature regarding how electronic devices are considered and treated in Fourth Amendment law.

This chapter also presented the border search doctrine, its statutes, and case law, including how electronic devices and their search at the border were viewed under the doctrine prior to *Riley*. This chapter also set forth how this thesis seeks to answer the twin research questions.

Chapter II analyzes the impact of *Riley* and conducts a detailed review of the Fourth Circuit's decisions in *Kolsuz* and *Aigbekaen*. It examines how other lower courts have split the on the question of electronic border searches including the reasonable object and manner of such searches. Chapter II discusses the use of forensic tools in electronic border searches and analyzes how courts have diverged in their definitions of what constitutes reasonable suspicion in the search of electronic devices at the border. Chapter II also explores the *Riley* decision itself and suggests that its applicability to searches of electronic devices at the border is extremely limited.

Chapter III introduces a new perspective for considering electronic devices at the border—a hybrid view. A model that attempts to stake out a middle ground between views that define electronic devices as entirely containers and those which declare them to be an entirely a new kind of property deserving of a special category of rules. In doing so, Chapter III first examines other areas of search and seizure law where perspectives akin to the hybrid model have evolved to balance significant government interests and important privacy concerns. The chapter then looks to existing statutory regimes, like the Electronic Communications Privacy Act and the Bank Secrecy Act, for support for the hybrid model. Chapter III also discusses the benefits of the hybrid model from its neutral treatment of different forms of property, the mode in which property transits the border, to its ability to adapt to changing privacy attitudes. Also examined is how the problems of bright-line rules are avoided by assuming a hybrid perspective of electronic devices at the border. Chapter III then closes by discussing how the hybrid model, by viewing electronic devices as both containers and novel property, allows for the protection of data that does not implicate historic government border interests. Specifically, this chapter explores how the hybrid model respects individual privacy interests in such data by treating that data as novel effects beyond the reach of suspicion-less searches by customs officers.

Chapter IV presents a tiered, hybrid-scope-limited approach for electronic border searches. As part of this presentation, the chapter examines how other scope-limited approaches have been implemented for searches where compelling government needs and individual liberty collide. Among the areas discussed that involve scope-limited approaches are searches of vehicles incident to arrest (SIA-Vs) as well as protective frisks and sweeps. Chapter IV then defines the tiered framework of this approach by outlining a two-tiered concept for electronic border searches linked to disparate levels of suspicion. In discussing the proposed two tiers of electronic border searches the reasonableness of forensic searches of electronic devices when customs officers are armed with an increased level of suspicion is examined. Chapter IV concludes by demonstrating why reasonable suspicion in line with the Supreme Court's definition in *Terry v. Ohio* is preferable to other, novel definitions justifying second-tier electronic border searches.

Chapter V discusses how a tiered, hybrid-scope-limited rule maintains the desired balance between government interests and personal privacy at the border. It answers the question as to whether the practice of searching electronic devices at the border continues to be constitutional following the *Riley* decision. It also answers the question as to how the reasonableness of this practice can be maintained in the future in the face of evolving technology through the application of a tiered, hybrid-scope-limited approach. Chapter V then provides conceptual guidance for customs officers undertaking electronic border searches, in accordance with this approach, as they confront the unique issues that modern electronic devices present.

II. THE IMPACT OF *RILEY* ON ELECTRONIC BORDER SEARCHES

Riley v. California did not involve border searches.[94] But *Riley*'s explication of privacy issues stemming from searches of modern cellular phones has ignited a debate that has spread to the question of electronic border searches. Specifically, *Riley* presents a challenge to the constitutional reasonableness of such searches, without suspicion or warrant, even when government interests reign supreme.[95] This chapter explores the application of *Riley*'s rationale to electronic border searches in *U.S. v. Kolsuz* and its progeny, *U.S. v. Aigbekaen*. This chapter then highlights the divergences that have occurred between Courts of Appeal in determinations concerning the object and manner of electronic border searches as well as disparate definitions of reasonable suspicion. Lastly, this chapter more closely examines the *Riley* decision itself, its nuances and its verbiage, and how its categorical rule for SIA searches is distinguishable from electronic border searches. Ultimately, this chapter reasons that while *Riley* does call for a rethinking of electronic devices as property, the decision and its rationale should not signal the demise of electronic border searches.

A. APPLYING *RILEY*'S NOVEL VIEW OF ELECTRONIC DEVICES AT THE BORDER: *U.S. V. KOLSUZ*

In light of *Riley*, the Fourth Circuit became the first to apply the High Court's data exceptionalist arguments to the border search context.[96] In *Kolsuz*, the court reviewed a forensic border search of a smartphone carried by a traveler attempting illegally to export firearm components in his checked baggage.[97] The court reasoned that the forensic analysis of the traveler's smartphone constituted a deeper invasion of privacy than a manual (user

[94] *Riley*, 573 U.S. 373.

[95] The Fourth Amendment of United States Constitution states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

[96] "The Border Search Muddle," 2280–81.

[97] *Kolsuz*, 890 F.3d at 138–39.

interface) search.[98] Often citing *Riley*, the *Kolsuz* court rejected the equation of electronic devices with other physical containers crossing the border.[99] Applying *Riley*'s reasoning, the court fashioned a rule that declared that electronic devices are a different type of property and that the information they contain is "uniquely sensitive."[100] *Kolsuz*, therefore, established a tiered standard that requires particularized and individualized suspicion for any electronic border search beyond a manual (user interface) search.[101]

More broadly, the *Kolsuz* court wrote that electronic border searches are only reasonable if "relevant government interests are present."[102] The court noted that reasonableness is a function of the historically recognized purposes and justifications for the border search doctrine itself.[103] In other words, electronic border searches must be undertaken for effecting those over-arching government interests at the border that have been defined as protecting national security, preventing the introduction of harmful goods, preventing illegal immigration, and generating revenue.[104] Thus, electronic border searches targeting terrorism, the smuggling of sensitive technology, and the cross-border movement of different types of contraband, for example, are constitutionally reasonable. But *Kolsuz* drew a line there.[105] The court wrote that electronic border searches conducted for "generalized law enforcement purposes" or "combatting crime" would not reasonable because they diverge from "the rationale for the border search exception" itself.[106]

---

[98] *Kolsuz*, 890 F.3d at 145–46. A manual (user interface) search is a search conducted by hand, without the assistance of special computer equipment or programs, to inspect the contents of a device. The customs officer during the search can see only the data that are visible to other device users and in the same format that other users see the data.

[99] *Kolsuz*, 890 F.3d at 145–46.

[100] *Kolsuz*, at 145.

[101] *Kolsuz*, at 146–47.

[102] *Kolsuz*, at 142.

[103] *Kolsuz*, at 143.

[104] Carroll v. United States, 45 S. Ct. 280, 302 (1925); *Ramsey*, 431 U.S. at 616; *Montoya de Hernandez*, 473 U.S. at 537–38.

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

[106] *Kolsuz*, at 143.

Kolsuz's foremost implication for searches of electronic devices at the border is that while they have great latitude, they are not "boundless."[107] While the *Kolsuz* acknowledged all electronic data could be searched at the border, it was the first appellate court to impose restrictions related to substantive scope. Constitutional reasonableness then hinges on whether the customs officer's action was tethered to those large categories of sovereign interest for which the border search doctrine was originally created to protect. In particular, reasonableness depends on "ongoing" and "transnational" threats that trigger the weighty interests of the sovereign at the border.[108]

Subsequently, in *U.S. v. Aigbekaen*, a case involving forensic electronic border searches grounded on suspicions of domestic human trafficking activity, the Fourth Circuit found forensic searches of a laptop and smartphone to be an unreasonable application of border authority due to the lack of relation between the suspected offense and the U.S. nation-state's border interests.[109] Echoing *Kolsuz*, the *Aigbekaen* court stated the border search exception, like all other Fourth Amendment exceptions, "should be defined by its justifications."[110] Significantly, the court noted it is not the "search's *location* [that] is . . . dispositive" but "rather, it is the search's relation to the [g]overnment's *sovereign interests* that is paramount" (original emphasis).[111] In this regard, the *Aigbekaen* court identified only the four very broad categories recited in *Kolsuz*.[112] It did not reach questions of standards for manual (user interface) searches, noting that the government lacked a particularized, individualized suspicion of an offense that "[bore] some nexus to the border

[107] United States v. Aigbekaen, 943 F.3d 713, 720 (4th Cir. 2019).

[108] *Kolsuz*, 890 F.3d at 143–44.

[109] *Aigbekaen*, 943 F.3d at 723. The judgment was affirmed based on the good-faith exception.

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

[111] *Aigbekaen*, at 722.

[112] *Aigbekaen*, 943 F.3d at 721. In referencing *Kolsuz* and citing *Ramsey*, the *Aigbekaen* court phrased the core sovereign interests underpinning the border search exception as "protecting national security, collecting duties, blocking the entry of unwanted persons, and disrupting efforts to export or import contraband."

search exception's purposes."[113] Thus, "no reasonable basis" existed for suspecting the trafficking crimes included a "transnational component."[114]

B. CIRCUIT SPLIT EMERGES

The *Kolsuz*, and *Aigbekaen* rulings constituted a significant break with border search precedent. Some courts have refused to go along in this direction based on border search supremacy arguments, some of which are enunciated in Supreme Court precedent, tethered to statutory regimes both old and new. Other courts have gone further than the *Kolsuz-Aigbekaen* rules to limit the application of the border search doctrine to electronic devices, focusing on individual privacy interests rather than earlier decisions or statutory history. Still others, unsure of the impact of *Riley*, have hesitated in making definitive declarations. Accordingly, no clear judicial consensus exists as to the reasonableness and constitutional permissibility of electronic border searches since *Riley*.

Rather, battle lines between competing viewpoints have centered three aspects of electronic border searches. First, courts have disagreed on the appropriate objects of electronic border searches or exactly what customs officers can search in the data contained in an electronic device. Second, courts do not agree on manner of search; specifically, the circuits diverge in their conclusions as to the reasonableness of manual (user interface) electronic border searches and forensic electronic border searches. Third, courts have articulated different definitions of "reasonable suspicion" in their electronic border search discussions. This section covers these areas and the divergent arguments about them in their turn.

1. The Object of Electronic Border Searches

The border search statutes authorizing customs searches are well-established and exceedingly broad. No property has ever been legislatively placed beyond the bounds of a lawful border search. The Supreme Court has repeatedly articulated the plenary nature of the doctrine in that all that crosses the border, regardless of its character, is subject to

[113] *Aigbekaen*, 943 F.3d at 721.

[114] *Aigbekaen*, at 721.

search.[115] Thus, historically, only one requirement emerged from this legal foundation for border searches to be reasonable: merchandise—"goods, wares, and chattels of every description."[116] Specifically, either the object of the search is merchandise or the object may contain merchandise or evidence of it.[117]

Given that searches for merchandise at the border have long been defined as encompassing all manner of property encountered there as subject to unbridled search, some courts have refused to follow the rationale of *Kolsuz* and *Aigbekaen*. The Eleventh Circuit in particular has found that electronic devices are merchandise and capable of containing merchandise, like all other items of property, and that customs officers have the prerogative to search them and the data they contain. In so finding, that circuit has reasoned simply that electronic border searches "are not embraced within the prohibition of the Fourth Amendment."[118] Rather, that circuit has held—even after *Riley* and *Kolsuz*—that any type of property can be searched at the border "simply by virtue of the fact that [the search] occur[s] at the border."[119]

Other courts have gone further than *Kolsuz* and *Aigbekaen* and taken a much narrower view as to when electronic devices and their data can be considered merchandise thereby subjecting them to reasonable search by customs officers. In 2019, for example, in *U.S. v. Cano*, a Ninth Circuit Court of Appeals decision, a three-judge panel ruled that electronic border searches had to be restricted only to the discovery of digital contraband; i.e., child pornography.[120] According to the court, denying the entry of digital contraband was the only rationale underlying customs authority at the border allowing for the search of a traveler's devices and data.[121] This narrow view is without foundation in previous

[115] See *Ramsey*, 431 U.S. at 616.

[116] 19 U.S.C. § 1401(c).

[117] Robles, *Law Course*, 159; 19 U.S.C. § 482.

[118] *Touset*, 890 F.3d at 1232. As background, the Eleventh Circuit encompasses the states of Georgia, Florida, and Alabama. The Fourth Circuit, which issued the decisions in *Kolsuz* and *Aigbekaen*, includes Virginia, Maryland, West Virginia, North Carolina, and South Carolina.

[119] *Touset*, 890 F.3d at 1232.

[120] *Cano*, 934 F.3d 1002. As background, the Ninth Circuit encompasses Alaska, Washington, Idaho, Montana, Oregon, Nevada, California, Arizona, Hawaii, Guam, and the Northern Mariana Islands.

[121] *Cano*, 934 F.3d at 1018–19.

border search case law or statute. The decision also ignored the statutorily established definition of merchandise which includes not just contraband but all other "goods, wares, and chattels."[122]

Still another court, two months after the *Cano* decision—hearing a civil case involving multiple plaintiffs suing the Department of Homeland Security and separate agencies with customs authority—adopted the most restrictive interpretation as to what customs officers may search for within electronic devices at the border.[123] In *Alasaad v. McAleenan* (aka *Alasaad v. Nielsen*), the district judge ruled that customs officers' suspicion-less electronic border searches must be restricted to turning on electronic devices and verifying that the devices contain data.[124] From there, according to the court, additional suspicion was necessary to search the data.[125] Except for digital items related to depictions of child pornography, these decisions flatly deny that electronic devices and data fall within the broad definition of merchandise. They distinguish all data from the large swaths of other, physical forms of merchandise based on form alone, ignoring substance. Accordingly, these decisions stand in direct conflict with other appellate case law.[126] In the end, these decisions symbolize, and contribute to, the current judicial disarray surrounding the object of permissible electronic border searches.

2. Manner of Search: Manual (User Interface) vs. Forensic Searches

The rift in the judiciary concerning electronic border searches has widened based on the manner of search as well. Before *Riley*, most courts accepted that any non-destructive searches of electronic devices and data at the border were reasonable no matter how they were conducted.[127] Since *Riley*, however, courts now disagree as to the

---

[122] 19 U.S.C. § 1401(c); Robles, *Law Course*, 159.

[123] *Alasaad*, No. 17-cv-11730-DJC.

[124] *Alasaad*.

[125] *Alasaad*.

[126] See United States v. Irving, 452 F.3d 110 (2nd Cir. 2006); *Kolsuz*, 890 F.3d 133; *Aigbekaen*, 943 F.3d 713; *Wanjiku*, 919 F.3d 472; *Cotterman*, 709 F.3d 952; United States v. Vergara, 884 F.3d 1309 (11th Cir. 2018); *Touset*, 890 F.3d 1227; and United States v. Molina-Isidoro, 884 F.3d 287 (5th Cir. 2018).

[127] *Cotterman* was the only pre-*Riley* court to adopt a different rule as to the manner in which electronic devices could be searched at the border.

circumstances under which a user interface or forensic electronic border search may be conducted.

a. What Is a Forensic Search?

While a user-interface search involves only a search of a device's data using the human eye, with a customs officer interacting with the device as would any user, a forensic search of an electronic device involves the use of special computer programs. Computer programs like Cellebrite, Encase, the Forensic Tool Kit and others allow for the creation of a "bitstream" copy of all of the data contained on a particular device, also known as the target device.[128] Making a bitstream copy involves more than just copying files.[129] These specialized forensic software applications allow for the copying of every byte of memory from a target device.[130] This includes data that can be seen and accessed by a user of the target device as well as data that is otherwise not visible to a user, like deleted files and metadata.[131] During the forensic process, this bitstream copy of data on a target device is transferred to another device under the control of the forensic examiner.[132] As the bitstream copy is created, it mirrors how the copied data is stored on the target device itself.[133] In this manner, the forensic search process prevents any alteration to the original data and the bitstream copy once made.[134] Accordingly, any future manipulations; i.e., search, of the copied data cannot alter either that copy or the original data.

---

[128] Kerr, "Searches and Seizures in a Digital World"; Sean E. Goodison, Robert C. Davis, and Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence* (Santa Monica, CA: RAND Corporation, 2015), https://www.rand.org/pubs/research_reports/RR890.html; Nikita Rana et al., "Taxonomy of Digital Forensics: Investigation Tools and Challenges," Cornell University, accessed November 22, 2020, https://arxiv.org/ftp/arxiv/papers/1709/1709.06529.pdf.

[129] Kerr, "Searches and Seizures in a Digital World," 541.

[130] Kerr, 541.

[131] Kerr, 541–42.

[132] Kerr, 540. The forensic process allows for "off-device" searches, i.e., searches of data that do not disturb the original device and are conducted on independent devices from where the bitstream copy has been transferred.

[133] Kerr, "Searches and Seizures in a Digital World," 540–41.

[134] Kerr, 540–41.

The use of forensic tools vastly enhances the thoroughness of an electronic device search.[135] Through this forensic process, government searches are more thorough and effective as they counter attempts to hide or erase evidence of crime, a capability that is constantly being afforded by the evolving technology behind modern electronic devices.[136] They can reveal files a user deleted and attempted to remove from a device's memory.[137] This search technique, however, also allows for searches of data that a user may be unaware his device is creating and storing.[138] Therefore, searches with forensic tools widen the physical scope of electronic device searches. A scope that is much broader than mere user-interface searches.

b. The Courts and Forensic Electronic Border Searches

Because of the enhanced search capabilities afforded by forensic software tools, some courts have crafted a reasonable suspicion standard for forensic electronic border searches.[139] Meanwhile, others have maintained that non-destructive searches of property at the border never require any amount of suspicion, no matter how they are conducted.[140] In particular, *Kolsuz* and *Aigbekaen* have kept to the suspicion-less rule for border searches involving a customs officer's visual inspection of data present on a traveler's electronic device. With respect to forensic searches, however, these courts have found that something more than zero suspicion is required. They have justified the higher standard for forensic searches due to their vast ability to increase the thoroughness of data searches.[141] Such searches capture more information including data of which that the traveler may be unaware or material that the user has sought to remove from a device.[142]

---

[135] Kerr, "Searches and Seizures in a Digital World," 541; *Aigbekaen*, 943 F.3d at 718.

[136] See Clancy, "Fourth Amendment Satisfaction," 44.

[137] Kerr, "Searches and Seizures in a Digital World," 542.

[138] Kerr, 542.

[139] *Cotterman*, 709 F.3d 952; *Kolsuz*, 890 F.3d 133.

[140] *Vergara*, 884 F.3d 1309; *Touset*, 890 F.3d 1227.

[141] *Kolsuz*, 890 F.3d at 145–46; *Aigbekaen*, 943 F.3d at 718.

[142] *Cotterman*, 709 F.3d at 965.

Conversely, the Eleventh Circuit, has repeatedly affirmed that a border search of an electronic device requires no additional suspicion, manual or otherwise. In *U.S. v. Vergara*, for example, after evaluating the impact of *Riley*, it rejected the application of a higher standard in forensic searches of electronic devices at the border.[143] Specifically, the *Vergara* court wrote "searches at the border, 'from before the adoption of the Fourth Amendment,' have been considered *reasonable* by the single fact that the person or item in question had entered into our country from the outside" (emphasis added).[144] The *Vergara* court invoked *Riley*'s clear edict limiting that holding solely to the province of SIA jurisprudence.[145] The court also cited *Riley*'s plain language that a cellular phone may still be searched pursuant to other recognized constitutional exceptions.[146] Whether electronic border searches are manual or forensic, in *Vergara*, was immaterial.

Less than 20 days following the opinion in *Kolsuz*, the Eleventh Circuit re-affirmed its decision in *Vergara*.[147] In *Touset v. United States*, the court stated pointedly "Property and persons are different."[148] According to the decision, "dignity and privacy interests," in the context of border searches, are only of concern when discussing "highly intrusive searches of the person."[149] Still the *Touset* opinion intoned that "import restrictions and searches of persons or packages at the national borders rest on different considerations and different rules of constitutional law from domestic regulations."[150] *Touset* concluded that regardless of the method used to search personal property, any non-destructive search of property at the border can be done without any degree of suspicion.[151]

Still other circuits have refused to align definitively with either the *Kolsuz-Aigbekaen* or *Vergara-Touset* view. In *U.S. v. Molina-Isidoro*, the Fifth Circuit avoided an

[143] *Vergara*, 884 F.3d at 1312.

[144] *Vergara*, at 1312.

[145] *Vergara*, at 1312.

[146] *Vergara*, at 1312.

[147] *Touset*, 890 F.3d 1227.

[148] *Touset*, at 1234.

[149] *Touset*, at 1234-35.

[150] *Touset*, at 1232.

[151] *Touset*, at 1233, 1236.

analysis of the reasonableness of user-interface and forensic electronic border searches and, accordingly, did not opine on a tiered approach to electronic border searches.[152] In noting the paucity of federal cases involving electronic border searches where some level of increased suspicion was required the court revealed its uncertainty in the application of such a requirement.[153] Then in March 2019, the Seventh Circuit Court of Appeals, in *U.S. v. Wanjiku*, followed a similar analytical path.[154] There, in reviewing the reasonableness of a forensic electronic border search, the court ruled that border search precedent confined the requirement for reasonable suspicion only to highly invasive searches.[155] The court specifically noted that the Supreme Court defined such searches as only those as related to "a person's most intimate body parts."[156] The court, however, did not expand the comparative analysis of user-interface and forensic electronic border searches for the purposes of articulating relative standards of suspicion required for each.[157] In November 2019, in *U.S. v. Williams*, the Tenth Circuit Court of Appeals similarly confronted the question of forensic electronic border searches.[158] Following the Fifth and Seventh Circuits, the court declined to find that reasonable suspicion was required to search "personal electronic devices at the border."[159] In particular, the court rendered no opinion on the bifurcated standard for user interface versus forensic electronic border searches adopted post-*Riley* by *Kolsuz*. Indeed, it avoided setting a standard altogether.

[152] *Molina-Isidoro*, 884 F.3d 287. As background, the Fifth Circuit includes Texas, Louisiana, and Mississippi.

[153] *Molina-Isidoro*, 884 F.3d at 293.

[154] *Wanjiku*, 919 F.3d 472. As background, the Seventh Circuit encompasses Wisconsin, Illinois, and Indiana.

[155] *Wanjiku*, 919 F.3d at 483.

[156] *Wanjiku*, at 485.

[157] *Wanjiku*, at 489.

[158] *Williams*, 942 F.3d 1187.

[159] *Williams*, at 1190.

3. Lack of Clarity in "Reasonable Suspicion" Standard

Before questions of electronic border searches arose, the reasonable suspicion standard was only applied to searches of property when the search was destructive.[160] Reasonable suspicion under the Fourth Amendment has generally been defined as particularized facts and circumstances indicating that "criminal activity [is] afoot."[161] This formulation is known as the *Terry* standard.[162] It applies within the borders of the United States to broaden law enforcement officers' ability to conduct limited searches and seizures when government law enforcement and safety interests are sufficient to justify some restriction on personal liberty.[163] Traditionally, the *Terry* standard had been reserved for highly invasive personal searches; i.e., strip or body cavity searches. By contrast all other border searches that were not dangerous, degrading, or damaging did not require the application of *Terry* to establish their reasonableness. Notably, no court has said that such warrantless, executive action by customs officers, supported by reasonable suspicion, at the border is unreasonable. To the contrary, the Supreme Court itself has stated that such border search activity is reasonable with far less than probable cause because of, among other things, the "the veritable national crisis in law enforcement caused by smuggling of illicit narcotics."[164]

After *Riley*, *Kolsuz* turned to the reasonable suspicion standard as the hurdle that customs officers had to clear in order to conduct forensic border searches. Specifically, *Kolsuz* returned to *Terry*'s "particularized" and "individualized" elements of the reasonable

---

[160] *Flores-Montano*, 541 U.S. 149. Destructive searches are "non-routine" border searches. Non-routine property searches, like non-routine personal searches, are more invasive and thorough than the cursory examinations at the border that a traveler may expect. For instance, while a traveler certainly should expect his property to be handled and examined at the border, he should not expect that it be destroyed. Several U.S. courts have set a fairly high standard for what are considered destructive searches of property requiring reasonable suspicion. Courts have allowed for the removal of door panels and gas tanks, cutting of spare tires, and drilling of holes in vehicles so long as property is still usable. See, for example, United States v. Cortez-Rocha, 383 F.3d 1093 (9th Cir. 2004); United States v. Chaudhry, 424 F.3d 1057 (9th Cir. 2005); and United States v. Cortez-Rivera, 454 F.3d 1038 (9th Cir. 2006).

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

[162] *Terry*, 392 U.S. 1.

[163] Thomas K. Clancy, *The Fourth Amendment: Its History and Interpretation*, 2nd ed. (Durham: Carolina Academic Press, 2014), 453.

[164] *Montoya de Hernandez*, 473 U.S. at 538.

suspicion analysis.[165] This paradigm was touted by several electronic border search observers even before *Riley*. But to *Kolsuz*, defining reasonable suspicion in the context of electronic border searches required that the suspicion be tethered to the justifications of the doctrine itself; in this case to thwart "ongoing transnational crime."[166] In doing so, it tightened the reasonable suspicion standard beyond *Terry*.

Since *Kolsuz*, several circuits that encountered the question of electronic border searches—and specifically, of forensic electronic border searches—have side-stepped or refused to delineate a detailed standard.[167] Instead, these courts have simply held that, however reasonable suspicion is defined, customs officers involved in the searches had the necessary suspicion to undertake reasonable forensic electronic border searches.[168]

Any understanding of what constitutes reasonable suspicion in the electronic border search context was thrown into further disarray with the Ninth Circuit's *Cano* decision. The court there found unreasonable the electronic border search of a cellular phone belonging to a traveler discovered to be attempting to smuggle 14 kilograms of cocaine in his vehicle.[169] Under other precedents, including *Kolsuz*, the discovery of the contraband merchandise would have constituted reasonable suspicion sufficient for a search of the phone, forensic or otherwise.[170] But the *Cano* court instead fashioned a new definition of what reasonable suspicion entails for border searches of electronic devices and data. Specifically, the court stated that reasonable suspicion in the context of an electronic border search was not linked to criminal activity but rather to a particularized, individualized suspicion that digital contraband was present on the device to be searched.[171] Shortly thereafter, the district court in *Alasaad* echoed the *Cano*'s rationale in finding that

---

[165] *Kolsuz*, 890 F.3d at 144.

[166] *Kolsuz*, at 144.

[167] See, for example, *Wanjiku*, 919 F.3d 472; Isidoro-Molina, 884 F.3d 287 (5th Cir. 2018); and *Williams*, 942 F.3d 1187.

[168] See, for example, *Williams*, 942 F.3d 1187.

[169] *Cano*, 934 F.3d at 1008, 1022.

[170] See *Kolsuz*, 890 F.3d 133; *Cotterman*, 709 F.3d 952; *Aigbekaen*, 943 F.3d 713; *Vergara*, 884 F.3d 1309; and *Touset*, 890 F.3d 1227.

[171] *Cano*, 934 F.3d at 1018–19.

reasonable suspicion justifying an electronic border search should be limited to digital contraband only.[172] Despite the broad historical justifications of the border search doctrine acknowledged in *Kolsuz*, these two decisions, set a truncated standard. One unconnected to existing statutes and caselaw and one that runs counter to statutory construction and repeated judiciary analysis; none of which has ever restricted reasonable suspicion searches at the border to only those related to contraband. To borrow from the writings of Judge Wilkinson in the *Kolsuz* decision, both cases "[build] a doctrinal house without foundation."[173]

C. DISTINGUISHING *RILEY* IN THE CONTEXT OF ELECTRONIC BORDER SEARCHES

Observers, like Laura Donohue, have argued that *Riley* rejects suspicion-less, warrantless electronic border searches of any kind as reasonable.[174] For multiple reasons, however, a wider application of that decision's rationale to the search of electronic devices pursuant to the border search doctrine is unsupportable. For one, border searches are an *exemption* to the Fourth Amendment, not an exception like SIA searches. In 2020, the Third Circuit Court of Appeals flatly stated that framing the border search doctrine as a mere exception is "an imperfect locution."[175] The court stated that categorizing the doctrine as an exception was erroneous as such terminology suggested it was "carved out from the Fourth Amendment's application."[176] Given the coetaneous birth of the doctrine and the Fourth Amendment, the court more accurately described searches at the border as "circumstance[s] in which the Fourth Amendment was never intended to apply."[177] *Riley*'s decision then to prevent the search of a cell phone under one Fourth Amendment exception

[172] *Alasaad*, No. 17-cv-11730-DJC at 37–38.

[173] *Kolsuz*, 890 F.3d at 153 (Wilkinson, J., dissenting).

[174] See Donohue, "Customs, Immigration, and Rights"; *Search and Seizure of Electronic Devices at the Border*: *Testimony before the Subcommittee on Federal Oversight Spending and Emergency Management of the Committee on Homeland Security and Governmental Affairs*, Senate, 105th Cong., 2nd sess. (2018) (statement of Laura K. Donohue), 23–25; and Park, "The Elephant in the Room," 303–6.

[175] United States v. Baxter, 951 F.3d 128, 131 n.7 (3d Cir. 2020).

[176] *Baxter*, at 131 n.7.

[177] *Baxter*, at 131 n.7.

within the borders of the United States has no bearing on the government's search of a cell phone, or any electronic device, at the border.

Furthermore, in addition to its long-established nature, the border search doctrine has a significant statutory basis. SIA searches have none. This fact was recognized by the Chief Justice in *Riley* when he declined to find electronic devices within the scope of SIA searches in the absence of any "precise guidance from the founding era."[178] With respect to the border search doctrine and electronic devices, there is both historical guidance and recent statutory support for electronic border searches. In the 21st century, Congress has explicitly contemplated and sanctioned the practice.[179]

Another significant factor limiting *Riley*'s application to electronic border search practice is the Court's plain language. While the Court disallowed SIA searches of electronic devices because the rationales supporting the SIA doctrine did not have "much force with respect to digital content on cell phones" if affirmatively restricted the breadth of its ruling.[180] In explicitly confining its holding to SIA searches, the *Riley* Court acknowledged that "other . . . exceptions may still justify" warrantless searches of electronic devices, including a cell phone.[181]

Further distinguishing *Riley* from the border search doctrine is the Court's certiorari decisions. The Court declined to hear an electronic border search case involving the same concerns related to warrantless searches of personal electronic devices and data, petitioned for certiorari at the same time as *Riley*.[182] In other words, the Court had the opportunity to limit the application of the border search doctrine to this type of property and advance the

[178] *Riley*, 573 U.S. at 376.

[179] 6 U.S.C. § 211.

[180] *Riley*, 573 U.S. at 376.

[181] *Riley*, at 386.

[182] "*Cotterman v. United States*," *SCOTUS Blog*, accessed July 9, 2020, https://www.scotusblog.com/case-files/cases/cotterman-v-united-states/. While *Cotterman* was rejected certiorari by the Supreme Court, it granted certiorari to review the *Riley* case and a companion case, *United States v. Wurie*. While *Riley* was taken for review out of the Ninth Circuit, the same circuit provided the *Cotterman* and later the *Cano* decisions. *Wurie* was a First Circuit case that arose from a district court case initiated in the District of Massachusetts, the same district that released the *Alasaad* opinion.

same "data exceptionalism" rationale.[183] But it declined to do so. Thus, while not explicitly exempting electronic border searches from scrutiny, the Court's strict limitations on the *Riley* holding, its reference to other exceptions allowing warrantless searches of electronic devices, and its certiorari choices strongly suggest that the Court meant to leave the border search doctrine, as applied to electronic devices, unchanged.

Furthermore, as much as *Riley* can be seen as a new paradigm for considering electronic devices as property, there is equal weight to the idea that *Riley* is about recalibrating SIA search doctrine to prevent the exception from becoming a loophole allowing warrantless "fishing expeditions."[184] Problems in reconciling SIA searches with the Fourth Amendment arose long before electronic devices, and SIA case law has evolved in fits and starts, sometimes with significant logical inconsistencies. [185] SIA searches have come to be accepted as allowing, "categorical[ly]," broad, general searches, without additional suspicion, for evidence of any crime.[186] Consequently, SIAs have become a warrantless "evidence-gathering technique" that effectively grants arresting officers a general search license because an officer need not have a "factual basis for believing" what type of evidence may be present.[187] Far from paralleling other constitutionally accepted warrantless search practices in the nation's interior, SIAs act, in important respects, not in

[183] "The Border Search Muddle," 2282–83.

[184] Ohio v. Robinette, 519 U.S. 33, 41 (1996) (Ginsburg, J., concurring).

[185] Clancy, *The Fourth Amendment*, 415–50. Clancy specifically notes, in juxtaposing the Supreme Court's decisions involving searches-incident-to-arrest of persons generally with those involving searches-incident-to-arrest of vehicles, that under the prevailing rule, a person "is more protected in an automobile than in his own home."

[186] Clancy, "Fourth Amendment Satisfaction," 53–54.

[187] Clancy, *The Fourth Amendment*, 448.

concert but in opposition to the Fourth Amendment and its requirements of specificity. A doctrinal problem exacerbated by the development of modern electronic devices.[188]

Issues surrounding cloud data storage were another concern of the *Riley* Court. The remote data access and storage capabilities of modern smartphones and applications troubled the Court if digital SIAs were to be allowed.[189] The Court feared digital SIAs could intrude onto data not present on a device and far exceed the scope of what can reasonably be searched in conjunction with an arrest.[190] The possibility of a search extending into property, even intangible data, far away from the location of arrest is anathema to the SIA doctrine. These concerns over unbounded intrusions into a person's digital life helped fuel the Court's ultimate prohibition of digital SIAs.[191] This danger, however, can be easily controlled in the border context. Users can isolate their devices from any cellular or wireless networks prior to inspection. The removal of this connectivity effectively prevents border search from extending into off-device data. It confines the border search to devices and their data that physically cross the border.

One other key difference between SIA searches and border searches is the number of practitioners authorized to exercise such extra-warrant search authority.[192] SIA searches can be conducted by any federal, state, or local government official with the power to

[188] Discussions concerning judicial decisions relative to SIA searches and their unique place within the Fourth Amendment construct are not complete without addressing the pretextual concerns some courts have. The idea that a person, no matter how significant or insignificant the crime, is exposed to the same general search activity allowed under the SIA doctrine has disquieted the High Court in both *Riley* and *Arizona v. Gant*. Just as with the *Riley* case, the facts in *Gant* presented the Court with questions regarding searches incident to arrest in the context of a relatively minor offense of operating a motor vehicle without a valid license. In that case, the Court significantly truncated the circumstances of an SIA vehicle search as well as its scope. As discussed in *Riley* and present by inference in *Gant*, the crime of operating a vehicle without a license for which both subjects had been arrested does not produce physical evidence that could be found on the subjects' persons or in the area proximal to the arrest. Through these decisions, the Court expresses its uneasiness over the pretextual nature of arrests for minor offenses, providing a loophole to conduct warrantless searches for evidence of other, more significant, criminality.

[189] *Riley*, 573 U.S. at 373–74.

[190] *Riley*, at 373–74.

[191] *Riley*, at 373–74.

[192] Clancy, *The Fourth Amendment*, 415–17. "Where one had been placed in the custody of the law by valid action of officers, the right to search the person incident to arrest is not unreasonable." United States v. Rabinowitz, 339 U.S. 56, 60 (1950). Accordingly, any official authorized to take a person into custody is authorized to exercise SIA authority.

undertake custodial arrests—a potentially huge pool of practitioners.[193] Attendant with these numbers is a large capacity for variances in the scope and conduct of SIA searches from case to case. Concerns regarding practice variances that include the potential for unreasonable search activity by practitioners is greatly lessened with border searches. Only federal government officials statutorily identified as customs officers have such authority.[194] Customs officers are present in only a few government agencies.[195] Thus, just as the area in which border search authority may be exercised is finite, so too are those empowered to effect such searches. The discreet number of insular practitioners decreases the chances of wide vagaries in application. Border searches then have the capacity to be more uniform and their reasonable conduct easier to delineate and discern.[196]

D. CONCLUSION

Riley has greatly upset the landscape where border searches of all property, including electronic devices, were once rarely questioned. The adoption of *Riley*'s rationale by *Kolsuz* and *Aigbekaen*, included a re-examination of the reasonableness of border searches of modern electronic devices in light of the rationale behind the government's broad authority at the border. But as part of this re-examination of border search authority across the judiciary since *Riley*, courts around the country have fundamentally disagreed as to how the doctrine reasonably applies to digital property and data. This disagreement involves divergent views as to what are the appropriate objects of electronic border searches. It also involves different views as to the manner in which electronic border

[193] *Rabinowitz*, 339 U.S. at 60.

[194] Robles, *Law Course*, 156–57.

[195] 19 U.S.C. § 1709 (2010); 19 U.S.C. § 1401(i); Robles, *Law Course*, 156–59.

[196] Additional factors distinguish the *Riley* decision and the SIA of electronic devices and electronic border searches. First, the *Riley* court specifically discussed the government's interest in searching electronic devices incident to arrest as being diminished by the fact that the threat of losing evidence contained in those devices is limited. Specifically, because the owner of the electronic device is being taken into custody, so too can that person's electronic devices. Accordingly, law enforcement officers can take custody of the devices or otherwise limit the mobility of the devices, their data, and any potential loss of evidence. This ability is not present in the border search context. People and property are not taken into custody as they transit national boundaries. Travelers and their property, including their electronic devices and stored data, are, in fact, quite mobile. As such, devices and data in which customs officers have an interest in searching can readily be carried away from the border; thus, such mobility frustrates the sovereign's ability to control what may enter and exit the country.

searches may be conducted; specifically, when such searches must be limited only to manual, user-interface searches and when customs officers may use forensic tools. There is so little consensus that across the judiciary several divergent definitions of what constitutes reasonable suspicion in the context of electronic border searches have been advanced. Despite the upheaval it has caused, however, a closer, detailed examination of *Riley* reveals that applying its rhetoric to the border search context is misguided because of the unique nature of the border search doctrine itself. *Riley*'s categorical approach to electronic devices in the interior is simply the wrong way to assess the continued constitutionality of electronic border searches and determine their reasonableness moving forward.

III. ELECTRONIC DEVICES AS HYBRID PROPERTY AT THE BORDER

Amid the dueling border search and data supremacy arguments that have characterized the post-*Riley* electronic border search debate, this chapter attempts to synthesize a middle ground. It presents a new perspective for electronic devices at the border: a hybrid view. The term "hybrid" is not explicitly used in search and seizure law but it is present by implication. That is to say, Fourth Amendment jurisprudence does recognize that certain property and situations have an inherent duality when government stakes and privacy stakes are simultaneously high.[197] In such instances, rigid application of bright-line Fourth Amendment rules tenets does not adequately serve the two. In short, a middle ground between plenary warrant requirements and blanket exceptions is necessary. This middle ground is often found when courts or legislatures tailor traditional principles to situations where the duality exists.[198]

A hybrid view or model of electronic devices at the border is a middle perspective because it avoids a view of electronic devices as entirely a container where all electronic data is considered a personal chattel (like a suitcase), subject to suspicion-less government review at the border. It also, however, refuses to view electronic devices as an entirely special class of property where even at the border the government has little authority to intrude. Instead, the hybrid perspective here accounts for the dual nature of electronic devices. It understands that electronic devices do contain data that is highly relevant to government interests at the border and substantively akin to physical property for which government border search authority is unquestioned. At the same time, however, the hybrid perspective accommodates the view that some data held in modern electronic devices is so unique, so personal, and so divergent from the border search rationale that it deserves protection from suspicion-less search.

---

[197] McAdams, "*Riley*'s Less Obvious Tradeoff," 119.

[198] Tailored rules are often more complex than categorical ones, but Richard McAdams notes that when "the stakes are high on both sides" of the government-interest versus personal-privacy debate, increased complexity is preferable because it affords optimization. See McAdams, "*Riley*'s Less Obvious Tradeoff," 120–21.

This chapter defines which digital content would be subject to a suspicion-less border search under a hybrid view of electronic devices. Then it elaborates on support for the hybrid view from situations were tailored rules have developed to deal with new technology or situations where the tension between personal privacy and legitimate government interests is high. This elaboration includes a discussion of the law involving motor vehicle searches, legislative enactment of the Electronic Communications Privacy Act, including language embedded Title III provisions, and the Bank Secrecy Act. All of these areas are similar to electronic border searches because while the personal privacy rights involved are significant the law has been tailored to accommodate extremely important government needs.

An examination of the benefits of a hybrid model for electronic devices follows, as well as a discussion concerning how a hybrid approach avoids problems created by categorical, bright-line rules. This chapter then closes by looking at specific items of modern electronic data that would be beyond the bounds of a suspicion-less border search under a hybrid view of electronic devices. In doing so, the chapter conceptualizes certain unique data as an "effect" and presents reasons for granting such data enhanced protection.[199]

A. DEFINING THE HYBRID VIEW: ELECTRONIC DEVICES AND THE BORDER

The hybrid view of electronic devices looks at their digital contents. First, it compares items of intangible data to traditional property. If an item of electronic data directly parallels tangible, physical property that is subject to search at the border, then the hybrid model holds that the electronic data is subject to suspicion-less border search. This would include documents and photographs stored digitally. Both have tangible property parallels which are subject to search if transported across the border in physical form. Second, if no traditional property parallel exists, the hybrid model assesses electronic data substantively. Specifically, it examines whether the nature of the data intersects the broad interests of the government at the border as they were defined in *Kolsuz* and *Aigbekaen*.

[199] U.S. Const., amend. IV.

An example of this would be recent call logs which do not have a directly comparable traditional property analog. Call logs, however, do reveal efforts to coordinate smuggling or trafficking activities. As such, if data does relate to the broad interests of the government at the border, regardless of the existence of a real-world comparison, the hybrid perspective still holds the data as being subject to a suspicion-less border search.

The hybrid model maintains consistency in the application of the border search doctrine. Data, no matter how new, is reasonably subject to search just like new types of physical property would be if they are relevant to recognized government interests at the border. The hybrid model, however, protects data that has no traditional property counterpart and, because of its nature, does not relate to government search interests at the border. An example of this type of data is stored internet search histories. Not only do digitally stored internet search histories not have a traditional property parallel, those records, on their face, are not capable of revealing information pertaining to such matters as national security, smuggling, or illegal immigration. Consequently, with respect to such novel data, the hybrid model precludes suspicion-less searches of that data by customs officers.

The hybrid model recognizes the significant legal basis authorizing the government to search for merchandise crossing the border.[200] It provides for the application of existing rules for searching merchandise in modern form. For instance, if a traveler carries a hard-bound book across the border, the volume would be subject to inspection by customs officers. Technically speaking, the book is merchandise. If instead of carrying the book in paper form a traveler carries its e-book counterpart across the border in a laptop computer or e-reader, the hybrid model provides for the reasonable search of that e-book. The text of book, regardless of form, is merchandise and subject to the same inspection because the content is the same.

The hybrid model for electronic devices at the border also accounts for the reasonable search of data that has no physical counterpart but that is still highly relevant to government interests. Text messages have no direct physical property parallel but can

[200] 19 U.S.C. § 482.

contain evidence of merchandise being moved across the U.S. border or be relevant to matters of national security.[201] Thus, the hybrid model too allows for their reasonable, suspicion-less search by customs officers at the border. By contrast, data generated by a smartphone application or a wearable fitness device, like a "fit-bit," that monitors a traveler's physical activity and some aspects of personal physiology have no real-world property comparison.[202] Moreover, such data does not touch on relevant government concerns. Under the hybrid model, customs officers would be precluded from conducting a suspicion-less border search of this data.

Importantly, the hybrid model is balanced. Just because a large amount of electronic data is subject to suspicion-less border searches does not mean that the government can search all data. The adoption of hybrid view of electronic devices allowing for the application of traditional search and seizure rules is not new. Such a model has basis in rules tailored to address other technological developments like those developed to define reasonable searches of motor vehicles.

B. CASE LAW SUPPORT FOR HYBRID APPROACH: THE *CARROLL* DOCTRINE

The mobile conveyance exception to the Fourth Amendment, first enunciated in *Carroll* is a hybrid property approach.[203] The *Carroll* Doctrine treats vehicles as hybrid property; that is property in which people have significant privacy interests but in which the government has concomitant interests that cannot be satisfied through rigid application of the Fourth Amendment's warrant tenet.[204] On the one hand, vehicles are personal effects and can hold highly personal highly personal property.[205] On the other hand, vehicles can rapidly and readily move thereby defeating the government's ability to affect searches with

[201] United States v. Modes, Inc., 787 F. Supp. 1466, 1475 (Ct. Int'l Trade 1992).

[202] Molly McLaughlin, "How Does a Fitbit Work?," Lifewire, February 22, 2020, https://www.lifewire.com/what-is-fitbit-4176010.

[203] *Carroll*, 45 S. Ct. 280.

[204] See *Carroll*, 45 S. Ct. 280; and California v. Carney, 471 U.S. 386 (1985).

[205] United States v. Jones, 565 U.S. 400 (2012); *Carney*, 471 U.S. 386.

a warrant. Vehicles can simply move across jurisdictions too quickly, outpacing the government's ability to obtain and serve a search warrant.

In addition to being a container, vehicles are also instrumentalities. Vehicles provided a new means for committing crimes. They are capable of both concealing and smuggling goods while also enabling individuals to commit crimes and escape the scene of those crimes.[206] The hybrid approach to motor vehicles, one that tailors established search and seizure precepts, is justified by the fact that vehicles are subject to larger levels of government control.[207] Specifically, the government can tax them, regulate their use on public roads, require registration, and also restrict how their owners may use them.[208] In short, the government has compelling interests in effecting searches of vehicles distinct from other property. But because of their unique characteristics, specifically their ability to defeat searches with a warrant, the Supreme Court in *Carroll* recognized the need to adapt traditional principles to searches of vehicles. To accommodate for the unique characteristics of vehicles, the Court tailored existing Fourth Amendment search rules by alleviating the problem of delays caused by the need for law enforcement to secure a warrant before conducting a search of a vehicle.[209] Instead, *Carroll* empowered law enforcement, armed with probable cause, to immediately proceed with a vehicle search without the possibility of losing that ability to search while awaiting a warrant.[210] The result is that the reasonableness of vehicle searches under *Carroll* are based only on the object of their search—namely, evidence of crime.[211] *Carroll*'s formulation then is an example of a tailored application of existing Fourth Amendment rules to account for the novel characteristics of what, nearly a century ago, was a new technology.[212]

---

[206] See *Carroll*, 45 S. Ct. 280; and Chambers v. Maroney, 399 U.S. 42 (1970).

[207] South Dakota v. Opperman, 428 U.S. 364, 368 (1976).

[208] *Carney*, 471 U.S. at 392–93. See also Cady v. Dombrowski, 413 U.S. 433 (1973).

[209] *Carney*, 471 U.S. at 390–91.

[210] *Opperman*, 428 U.S. at 367.

[211] United States v. Ross, 456 U.S. 798, 824 (1982).

[212] Importantly, this hybrid property view of motor vehicles is unaffected by the quantitative or qualitative nature of the personal effects a person stores therein. Even vehicles that act as a person's home—the most sanctified place in Fourth Amendment law—are subject to warrantless searches. See *Carney*, 471 U.S. 386.

The development of the *Carroll* doctrine is instructive in an analysis of electronic border searches in that vehicles were a revolutionary innovation in property that challenged existing constitutional precepts in many of the same ways modern electronic devices do.[213] Like motor vehicles, electronic devices too are readily mobile. They act as both containers and instrumentalities. They carry with them significant privacy interests. At the border, however, they and their data can implicate the same government regulatory interests as traditional property.[214] In assuming a hybrid perspective, like that implicitly used for motor vehicles, the quantity or private nature of the information electronic devices is not dispositive. Rather, as under *Carroll*, viewing electronic devices at the border as hybrid property ties the reasonableness of an electronic border search to the object of and rationale for the search.

C. OTHER STATUTORY SUPPORT FOR THE HYBRID MODEL

Electronic border searches under the hybrid model can intrude into digital privacy and, specifically, electronic communications, but this eventuality does not render searches consistent with the model unreasonable. Critics like Laura Donohue argue that the scope of electronic border searches need be truncated to protect electronic communications.[215] She compares electronic messages to postal mail and, in doing so, relies exclusively on restrictions to the examination of outbound mail in the custody of the U.S. Postal Service.[216] This rationale, however, ignores explicit and implicit statutory support for border searches encompassing communications, no matter the form in which they are carried. Specifically, border searches of inbound U.S. Mail, including correspondence, can be conducted by customs officers without restriction when they are suspected of containing or related to merchandise.[217] Moreover, correspondence carried in or out of the country by a traveler or private courier service, is not part of the mails, and is fully subject to suspicion-

[213] Kerr, "Foreword: Accounting for Technological Change," 407.

[214] Nowell, "Privacy at the Border," 85–104. See also Sales, "Run for the Border"; and Gilmore, "Preserving the Border Search Doctrine in a Digital World."

[215] Donohue, "Customs, Immigration, and Rights," 980.

[216] Donohue, "Customs, Immigration, and Rights," 980. See 19 U.S.C. § 1583 (2008).

[217] 19 C.F.R. §§ 145.2–145.3 (2012); Robles, *Law Course*, 178.

less examination by customs officers.[218] In addition, any argument seeking additional protections at the border for written communications, whether in physical or digital form, ignores the fact that searches of "envelopes" are specifically authorized at the border.[219] Apart from these border rules, further support for electronic communications, like other private data, being subject to electronic border searches, even under a hybrid view, can be gleaned from other statutory regimes.

1. Electronic Communications Privacy Act

Congress has recognized through its passage of the Electronic Communications Privacy Act (ECPA), the need for a middle ground to ensure the government has access to important evidence contained within new communications technology. The result is significantly diminished privacy protections for electronic communications (i.e., digital communications). [220] The ECPA allows for different ways in which the government may access stored electronic communications under given circumstances and that access does not in all cases require the protection of a search warrant.[221] While stored electronic communications held in a provider's electronic storage for less than 180 days require the government to obtain a warrant to search, such communications stored for 180 days or more do not.[222] In fact, such communications may be obtained by law enforcement with only a subpoena.[223] Transactional information, including identifying data of others with whom a particular subscriber has communicated, only requires a showing that such

[218] *Ramsey*, 431 U.S. at 620.

[219] Donohue, "Customs, Immigration, and Rights," 980; See 19 U.S.C. § 1583; 19 U.S.C. § 482; and 19 C.F.R. §§ 162.6–162.7.

[220] See, generally, "Electronic Communications Privacy Act of 1986 (ECPA)," Justice Information Sharing, April 23, 2019, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285. Passed in 1986, the ECPA is frequently used to refer to two pieces of legislation: 1) The Electronic Communications Act (ECA) proper and 2) the Stored Wire Electronic Communications Act (SCA). This legislation modernized the legal guidelines for the government's authority to obtain wire, oral, and electronic communications. It delineated the degree of protection afforded all communications whether they are in transit or otherwise stored on digital and electronic storage media including computers and computer servers.

[221] 18 U.S.C. § 2703(b) (2011).

[222] 18 U.S.C. § 2703(a).

[223] 18 U.S.C. § 2703(b).

information is "reasonable and material."[224] And even when a search warrant is needed, an ECPA warrant does not require the same intensive benchmarks as an order authorizing interception of spoken communications or even the live time interception of transcribed communications.[225] Even in the interior electronic communications only receive limited protection. The ECPA then, by its very construction, contradicts arguments that electronic communications should be granted elevated protection.[226]

The real-time communication monitoring provisions of the ECPA (often referred to a Title III) also serve as an important guidepost for the reasonableness of searching electronic communications during electronic border searches. These provisions set protection for electronic communications "at the Fourth Amendment standard of protection, rather than the additional level given . . . to oral and wire communications."[227] In fact, Congress explicitly provided in its legal formulation that electronic communications as a class are subject to the normal reasonableness and warrant rules developed under Fourth Amendment jurisprudence.[228] For instance, electronic communications do not receive the protection of real-time minimization like oral and wire communications do.[229] Thus, per statute, electronic communications do not receive special

[224] 18 U.S.C. § 2703(d).

[225] Kenneth Dam and Herbert Lin, eds., *Cryptography's Role in Securing the Information Society* (Washington, DC: National Academies Press, 1996), https://doi.org/10.17226/5131.

[226] In some respects, border searches are a more legitimate intrusion into electronic communications than those allowed under the ECPA. Under that legislation, the government may collect electronic communications, and even oral and wire communications, without any type of judicial authorization if one of the parties involved in the communication consents to the collection. This means that law enforcement acting wholly within the United States and dealing with internal crimes can reasonably obtain private communications without all parties being privy to their collection and without external oversight. Conversely, with electronic border searches, the traveler is aware when his electronic devices are being searched and knows the electronic communications contained on an electronic device may be reviewed pursuant to that search. Furthermore, unlike that provided by the ECPA provisions, government intrusions into electronic communications and data at the border can be circumscribed to some degree. The hybrid model can limit intrusions into communications that impact the "primordial purpose[s]" of the border search doctrine. See 18 U.S.C. § 2511(c) (2011); and United States v. Sahanaja, 430 F.3d 1049, 1053 (9th Cir. 2005).

[227] Dam and Lin, *Cryptography's Role in Securing the Information Society*, 401.

[228] Dam and Lin, 401.

[229] "Electronic Surveillance—Title III Affidavits," Department of Justice, February 19, 2015, https://www.justice.gov/archives/jm/criminal-resource-manual-29-electronic-surveillance-title-iii-affidavits.

protection and are like traditional property in assessing Fourth Amendment reasonableness.[230]

2. Bank Secrecy Act

The Bank Secrecy Act (BSA) is another statutory regime where, without much controversy, personal privacy interests, including those at the border, are explicitly and significantly diminished. Under the BSA, they are explicitly placed secondary to the government's interest in promoting the nation's security through greater power to counter currency generating threats, both foreign and domestic. Specifically, the BSA allows for government oversight of highly private currency transactions. The BSA does this through numerous reporting requirements including the "Report of International Transportation of Currency or Monetary Instruments."[231] This legislative requirement is a border search statute that mandates that any person who, among other things, "physical[ly] transports . . . currency . . . in an aggregate amount exceeding $10,000 into or out of the United States" files such a report.[232] It empowers customs officers to oversee what is being moved in and out of the country thereby enhancing border and national security.

Other BSA provisions also significantly enhance government authority at the expense of personal privacy. Specifically, the BSA requires all financial institutions to document qualifying currency transactions occurring within the United States and furnish the government with those records.[233] These provisions also require financial institutions to document any suspicious transactions.[234] Thus, despite the highly private nature of a person's currency and banking transactions the regulatory scheme adopted by Congress

---

[230] See, for example, 18 U.S.C. § 2518(10)(c) (2010), specifically about limiting judicial sanctions and remedies relative to the interception of electronic communications.

[231] Office of the Comptroller of the Currency, *Bank Secrecy Act/Anti-Money Laundering: Comptroller's Handbook* (Washington, DC: Office of the Comptroller of the Currency, 2000), 1, 7. The BSA is also known as the Currency and Foreign Transactions Reporting Act.

[232] 31 U.S.C. § 5316 (2011).

[233] "Bank Secrecy Act (BSA) & Related Regulations," Office of the Comptroller of the Currency, March 25, 2019, https://www.occ.treas.gov/topics/supervision-and-examination/bsa/bsa-related-regulations/index-bsa-and-related-regulations.html. See also 31 C.F.R. §§ 1010.300–1010.370 (2011).

[234] "Suspicious Activity Reports (SAR)," Office of the Comptroller of the Currency, March 4, 2019, https://www.occ.treas.gov/topics/supervision-and-examination/bank-operations/financial-crime/suspicious-activity-reports/index-suspicious-activity-reports.html. See also 31 C.F.R. § 1010.320.

allows the government to intrude significantly into the financial lives of individuals, within the United States, without the need for a warrant.[235] The legislatively created dynamic of the BSA that promotes government interests over those of the individual for sovereign security reasons is analogous to the border where significant invasions of privacy have too been recognized by statute. Unlike the BSA, however, the hybrid model for electronic devices and data at the border does allow for some restraints on government authority which afford some degree of privacy in a traveler's digital life.

D. BENEFITS OF HYBRID PROPERTY VIEW OF ELECTRONIC DEVICES

There are two important benefits to the adoption of a hybrid property perspective for electronic devices in the context of electronic border searches. The hybrid view provides a mechanism for mitigating the problem for border searches created in the wake of *Riley*; that is the creation of different rules for different forms of property. The hybrid view does not grant greater or lesser protection based typological property differences. It also does not bestow immunity from search based on the method in which the property item physically crosses the border. It is neutral in both respects. A second benefit from the hybrid model is that it provides for a measured approach preventing the government from rummaging through the entirety of a traveler's digital existence and history. As such, the model has the ability to adapt to changing privacy conceptions as well. The following sections discuss the hybrid model's favorability for its neutral rules and its fluidity to meet changing privacy attitudes.

1. Technological and Travel Mode Neutrality

Technological neutrality is important in maintaining consistency in search and seizure law and the border search doctrine. Noted Fourth Amendment scholar Orin Kerr has written that the constitutional balance struck in the physical world should be the same balance that is struck in the digital world.[236] Richard McAdams has argued that creating one set of rules for digital property and another for traditional property is a faulty

[235] See, for example, 31 C.F.R. § 1010.520 (2011); and 12 U.S.C. § 3413 (2010).

[236] Kerr, "Applying the Fourth Amendment to the Internet," 1017.

approach.[237] The creation of separate rules is another reason why, according to McAdams, *Riley*'s categorical approach to electronic devices is problematic as it widened "the gap between digital and 'analogue' searches."[238] Other Fourth Amendment scholars, like Thomas Clancy, have cautioned that creating a special property category with special rules for electronic devices threatens to create a two-track Fourth Amendment, one track for digital property and another track for all other property.[239] This could lead to the creation of ad hoc rules resulting in "stark" differences in how digital and traditional property are treated under the law, when in substance each are quite similar.[240]

At the border, technological neutrality is necessary to preserve the established dynamic granting the government broad search authority to protect the nation and people from harm. It is illogical to grant travelers increased levels of privacy simply by virtue of carrying their property in digital versus physical form.[241] When electronic devices act as containers holding in their memory an item that has a direct physical counterpart, no distinctions should be made. These items should be subject to examination at ports of entry and exit just as a tangible object. Some court's like *Cano*, in their haste to adopt *Riley*, violate the principle of technological neutrality. So unmoored from this principle was the *Cano* court that it *sua sponte* abrogated nearly all of Congress's definition of merchandise without even mentioning that statute let alone declaring it unconstitutional. It, in effect, created a special per se warrant rule only applicable to electronic devices at the border, and a child pornography exception to that warrant requirement. Decisions like that of *Cano*, and others, depict judges, creating special rules for digital property far adrift from accepted principle, "in over [their] heads," and ignorant of the dangers the border search doctrine has been established to counter.[242]

---

[237] McAdams, "*Riley*'s Less Obvious Tradeoff," 127–29.

[238] McAdams, 127.

[239] Clancy, "Fourth Amendment Satisfaction," 51.

[240] McAdams, "*Riley*'s Less Obvious Tradeoff," 128.

[241] *Touset*, 890 F.3d at 1233, 1236.

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

A hybrid view of electronic devices is valuable because it avoids separate categorical rules for different types of property. This view does not elevate form over substance in a manner that would render the government's border search authority "meaningless."[243] The hybrid view of electronic devices at the border refuses to exempt property from search only because of the form in which it is carried. The hybrid model preserves the cogency of border search rules by maintaining the desired balance between the government and individual at the border—that all property is subject to search—which should remain unchanged by the arrival of new technology.[244] The hybrid model is technologically neutral. It allows the government the same exercise of its long-standing sovereign right to interdict and uncover illicit cross-border activity no matter whether that activity is enabled by digital technology or not.

Mode of transportation neutrality is important as well. Whether an item is carried across the border on a traveler's person or transits the border by other means, the border search doctrine is agnostic. The *Ramsey* Court was clear on this point when it wrote "that there is nothing in the rationale behind the border-search exception which suggests that *the mode of entry will be critical*" (emphasis added).[245] The *Ramsey* Court, in denying any distinction between a letter crossing the border in a traveler's possession vice one sent via the mail, noted the "critical fact" to be "not that [envelopes] are brought in by one mode of transportation rather than the another."[246] To the Court, "it [was] their entry into [the] country from without it that [made] a resulting search 'reasonable.'"[247] Mode neutrality is an aspect of the debate universally unaddressed by critics of electronic border searches.

There is no favored method of import or export in the law. Congress has placed no categorical restrictions on searches of "goods, wares, and chattels of every description" based upon how property is transported.[248] Critics of electronic border searches base their

[243] Gilmore, "Preserving the Border Search Doctrine in a Digital World," 786.

[244] Kerr, "Applying the Fourth Amendment to the Internet," 1015–17.

[245] *Ramsey*, 431 U.S. at 620.

[246] *Ramsey*, at 607.

[247] *Ramsey*, at 607.

[248] United States v. Garcia Paz, 282 F.3d 1212, 1214 (9th Cir. 2002); 19 U.S.C. § 1401(c).

arguments solely on the perspective of a traveler and the personal smartphone or laptop he or she may be carrying.[249] The logic articulated by the *Ramsey* Court holds equally true for goods that enter the country in the carriage of travelers as those which enter as palletized cargo, in express courier parcels, or other unaccompanied shipments. The border search doctrine and any rule relative to searches of electronic devices occurring there need to encompass all that crosses the border. This neutrality in mode of carriage or transportation means that property owners can expect their electronic devices and data to be subject to the same search rules whether their device are in their pockets, in their baggage, in their vehicle, in an express courier parcel, or in a shipping container.

2. Privacy Interests and Privacy Attitudes

Conceptually, assuming a hybrid property perspective for electronic devices and their data enables electronic border searches to sustain their reasonableness and adapt to changing attitudes toward personal privacy. For instance, observers in the digital age have advocated for a shift in thinking about privacy in the Fourth Amendment context.[250] Kerr advocates that the advancement of technology requires a change in focus from "inside/outside distinctions" relative to expectations of privacy to "content/non-content distinctions."[251] Authors like David Sklansky, have assumed the view that privacy means the ability to seek refuge in a place where the government cannot go.[252] Hence, to Sklansky, the right to privacy means an ability to retreat into what he terms "zones of refuge."[253]

---

[249] See, generally, Donohue, "Customs, Immigration, and Rights"; Upright, "Suspicionless Border Seizures of Electronic Files," 291; Flipse, "An Unbalanced Standard," 851–74; Matthew B. Kugler, "The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study," *University of Chicago Law Review* 81, no. 3 (2014): 1165–1211; Alzahabi, "Should You Leave Your Laptop at Home?"; Fontecchio, "Suspicionless Laptop Searches," 266; Coletta, "Laptop Searches at the United States Borders"; and Wilson, "Laptops and the Border Search Exception to the Fourth Amendment."

[250] See, for example, David A. Sklansky, "Too Much Information: How Not to Think About Privacy and the Fourth Amendment," *California Law Review* 102, no. 5 (2014): 1069–1121; Pamela Samuelson, "Review: A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy," *California Law Review* 87, no. 3 (1999): 751–78, https://doi.org/10.2307/3481032; Paul Ohm, "The Fourth Amendment in a World without Privacy," *Mississippi Law Journal* 81, no. 5 (2012): 1309–56; and Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment."

[251] Kerr, "Applying the Fourth Amendment to the Internet," 1017–22.

[252] Sklansky, "Too Much Information," 1113.

[253] Sklansky, 1115.

Sklansky advocates for such a paradigm shift to reassess the reasonableness of a variety of modern government intrusions including the collection of digital and electronic information and even the use of confidential informants. First, the hybrid model for electronic devices at the border comports with the essence of Kerr's argument by focusing on substance vice form. Second, even under Sklansky's alternate, expansive view of privacy, however, the hybrid model is both reasonable and sustainable. Third, travelers would maintain their "zone of refuge" in data that does not, in its substance, align with other property considered merchandise and historically within the sphere of customs inspection.[254] Furthermore, travelers have the ability to protect their data privacy at the border with the evolution in personal electronic devices that has made them more "cloud-enabled."[255] Using cloud storage and cloud-based applications, travelers can create a "zone of refuge" by storing their data off-device.[256] Because electronic border searches, as advocated in the next chapter, based on the hybrid model can be limited in their scope, both physically and in content, travelers can place any data they wish beyond the bounds where the government can go at the border.

E. AVOIDING THE PROBLEM OF BRIGHT-LINE RULES

A categorical view of electronic devices, either completely in favor of the government's search authority or completely favoring individual privacy, does not promote an effective balance. A bright-line, all or nothing, resolution to the electronic border search question lacks necessary nuance. On the one hand, a bright-line rule like that of *Riley*, and to a large degree articulated in *Cano* and *Alasaad*, could "eviscerate" the border search doctrine.[257] On the other, a bright-line rule protecting the government's absolute right to search electronic devices despite the growing privacy interests travelers have in certain types of data is too rigid. Such a standard would invariably become increasingly brittle and unsupportable in the face of ever-evolving technologies. Donald Dripps has recognized the

[254] Sklansky, 1115.

[255] David Linthicum, "The Cloud and the Internet of Things Are Inseparable," InfoWorld, January 12, 2016, https://www.infoworld.com/article/3021059/cloud-and-internet-of-things-are-inseparable.html.

[256] Sklansky, "Too Much Information," 1113–15.

[257] *Aigbekaen*, 943 F.3d at 729 (Richardson, J., concurring).

problem with bright-line Fourth Amendment rules.[258] While they are determinant and provide clear lines to practitioners, they struggle to maintain legitimacy over time.[259] Such rules lack adaptability to deal with novel factual scenarios presented by such issues like those inherent to modern technology. The inflexibility of categorical rules either render them obsolete or force them to become untethered from accepted doctrine which triggers their perception as increasingly illegitimate.

An example can be seen in the evolution of searches of vehicles incident to the arrest of an occupant (SIA-Vs). Prior to 2009, a bright-line rule for SIA-Vs existed that allowed these searches to be conducted after the occupants had been removed from a vehicle and their access to its contents significantly impeded. [260] The bright-line rule even allowed SIA-Vs to be conducted after an arrested occupant was locked in a law enforcement vehicle and even after they were taken from the scene of the arrest. [261] This bright-line rule, however, extended far beyond the original rationale for SIA-Vs. This unprincipled extension threatened the legitimacy of SIA-Vs. In *U.S. v. Gant*, the Supreme Court, though not using the terminology, returned to a hybrid model consistent with *Carroll*.[262] In doing so, it limited the circumstances in which the government can exercise SIA-V search authority.[263] The Court in *Gant* eschewed a categorical rule that gave the government plenary authority over vehicle while also protecting established government interests stemming from the unique technological character of motor vehicles. Thus, through a hybrid approach, *Gant* accounted for concerns on both sides of the categorical debate. A hybrid approach to modern electronic devices and their data at the border can strike a similar balance, thereby promoting the legitimacy of electronic border searches.

[258] Donald A. Dripps, "The Fourth Amendment and the Fallacy of Composition: Determinacy versus Legitimacy in a Regime of Bright-Line Rules," *Mississippi Law Journal* 74 (2004): 341–427.

[259] Dripps, 346–47.

[260] New York v. Belton, 453 U.S. 454 (1981).

[261] See Arizona. v. Gant, 556 U.S. 332, 341–343 (2009).

[262] *Gant*, at 343.

[263] *Gant*, at 343.

F. NOVEL ELECTRONIC DATA AS PERSONAL "EFFECTS"

Since the time of the Founding and until relatively recently, "effects" have been forgotten aspect of Fourth Amendment law.[264] Instead, the focus of many arguments against government warrantless property searches (including digital searches) have been based on claims that such searches violate personal privacy because they unreasonably invade a person's "papers."[265] The debate over the constitutionality of searches of papers has a long history and has occupied judges and scholars alike.[266] And some border search critics have advanced arguments questioning the reasonableness of electronic border searches rooted in the historic protection afforded personal papers.[267] Still others have examined the reasonableness of customs searches of private papers in light of the history of the border search doctrine and have not reached any definitive conclusions.[268] But relying on arguments that focus on privacy in papers is not helpful in defining a reasonable approach to electronic border searches. Papers have long been considered personal chattel.[269] As a chattel, their search is supported by statute and historically accepted.[270] Moreover, because "papers" in digital form either are directly comparable to or substantively parallel physical papers, arguments seeking to curtail electronic border search on these grounds are illogical; especially when they are unaccompanied by an argument favoring a prohibition on customs searches of physical papers.

---

[264] Maureen E. Brady, "The Lost 'Effects' of the Fourth Amendment: Giving Personal Property Due Protection," *Yale Law Journal* 125, no. 4 (2016): 948, 957.

[265] Donald A. Dripps, "'Dearest Property': Digital Evidence and the History of Private 'Papers' as Special Objects of Search and Seizure," *Journal of Criminal Law and Criminology* 103, no. 1 (2003): 49–110.

[266] Dripps, "Dearest Property"; "The Border Search Muddle," 2293–97. See also Thomas K. Clancy, "The Framers' Intent: John Adams, His Era, and the Fourth Amendment," *Indiana Law Journal* 86 (2011): 979–1617.

[267] See Donohue, "Customs, Immigration, and Rights."

[268] "The Border Search Muddle," 2293–97.

[269] As described by Lord Camden in an English Common Law case, "Papers are the owner's goods and chattels." Entick v. Carrington, 19 Howell's State Trials 1029, 1066 (CP 1765), quoted in "The Border Search Muddle," 2296.

[270] 19 U.S.C. § 1401(c); Robles, *Law Course*, 159, 178–79.

Conceptualizing certain electronic data that is wholly distinctive in both form and substance from other property as a novel "effect" is more useful in the context of ensuring reasonable electronic border searches.[271] What constitutes a personal effect has not been well defined by courts.[272] The term, however, has been used to encompass electronic devices as personal possessions.[273] It should also be used when considering certain types of modern data contained in those devices. According to Clancy, effects are personal possessions "implicating [a] person's reasonable expectation of privacy."[274] Effects, however, do have other definitions. In particular, *Black's Law Dictionary* provides a legal definition for an "effect" as a noun as "that which is produced by an agent or cause" or a "result" or "consequence."[275] Thinking of some electronic data as an effect recognizes that modern electronic devices and software applications are personal agents that produce information caused by or a consequence of their use. This kind of data; i.e., a novel digital effect, is a traveler's personal possession; one in which privacy is undoubtedly expected and that almost invariably has no physical world comparison. In addition, data considered an effect under this definition is irrelevant to the government's core border interests.

The category of novel digital effects here would include new types of digital information like electronic metadata that is created by electronic devices or software through their use and operation.[276] Also included would be data created as a result of modern electronic devices, like smartphones, acting as an agent involved in the monitoring of a user's physical health and activity. Information related to a user's internet search habits, movements, and proclivities would also be considered a novel digital effect. Data of this nature can be characterized as digital surveillance data and is created and stored

---

[271] U.S. Const., amend. IV.

[272] Brady, "The Lost 'Effects' of the Fourth Amendment," 960.

[273] Clancy, *The Fourth Amendment,* 190.

[274] Clancy, 189.

[275] Henry C. Black, Joseph R. Nolan, and Jacqueline M. Nolan-Haney, *Black's Law Dictionary: Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern*, 6th ed. (St. Paul, MI: West Publishing Group, 1990), 514.

[276] "Digital Evidence Metadata," CaseGuard, accessed October 5, 2020, https://caseguard.com/evidence-blog/digital-evidence-metadata. This source describes metadata as data that provide details about other data and are hidden within the electronic files of that data.

automatically on a device, often in a manner opaque to the user. Digital surveillance data is both highly revealing about a person's life and its creation and storage is frequently beyond the user's control.[277] For instance, many modern mobile phone applications specifically need to track a user's movements through a smartphone or other smart device in order to afford full functionality.[278] Consequently, rather than viewing this data as merchandise a traveler voluntarily carries across the border, the hybrid approach views this data as novel digital "effects" at the border.[279] In doing so, the hybrid perspective protects this special category of personal data from suspicion-less government trespass.[280]

The hybrid model's view of certain digital information created by new technology as a novel personal effect has received recent implicit support. The term "effect" returned to Supreme Court search and seizure jurisprudence in *U.S. v. Jones*.[281] This case centered on the use of GPS tracking technology in connection with motor vehicles.[282] Data produced as a consequence of the use of such technology was recognized by members of the Court as revealing significantly detailed information about a person's movements.[283] Though the *Jones* Court did not explicitly define that data produced by GPS vehicle trackers as a personal "effect," the re-introduction of this term in the context of one of the Court's cornerstone decisions concerning new technologies is insightful.[284] The insight is especially strong considering the implication of data as a personal "effect" in a case where many Justices agreed that the data trespass at issue allowed for an unreasonable privacy

[277] Cameron F. Kerry, "Why Protecting Privacy Is a Losing Game Today—and How to Change the Game," Brookings, July 12, 2018, https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

[278] Todd Haselton, "Many Apps on Your Phone Are Tracking Everywhere You Go—Here's How to Stop Them," CNBC, December 12, 2018, https://www.cnbc.com/2018/12/12/how-to-stop-apps-from-tracking-your-location.html.

[279] Brady, "The Lost 'Effects' of the Fourth Amendment," 976. This discussion relates to "trespass to effects" tests.

[280] Brady, "The Lost 'Effects' of the Fourth Amendment," 971.

[281] Brady, 957.

[282] *Jones*, 565 U.S. 400.

[283] *Jones*, at 415–16 (Sotomayor, J., concurring).

[284] Brady, "The Lost 'Effects' of the Fourth Amendment," 955, 957.

invasion empowering the government to create a detailed "mosaic" of a person's life.[285] Support for the idea of modern electronic data as a personal effect grew when the late Supreme Court Justice Antonin Scalia indicated that such a conceptualization might be a way to balance government interests and personal privacy in searches of data.[286] By viewing certain types of modern electronic data as novel digital effects, the hybrid model adapts the *Jones* "trespass test" to protect specially categorized data at the border.[287]

G. CONCLUSION

Treating electronic devices as hybrid property resolves the increasing tension between categorical perspectives in the electronic border search debate. The hybrid model takes a balanced view and promotes reasonableness by recognizing that while much electronic data should be subject to electronic border searches, special types of modern data should not be. Allowing data, directly paralleling tangible property, to be searched promotes technological neutrality and consistency in the application of border rules. Similarly, allowing the search of data, though entirely novel but still relevant to the issues giving rise to the government's broad border authority, is also legitimate. Such a data-centric focus looks at substance vice form. But the hybrid model draws a line. It also acknowledges that some data is so novel that it cannot fairly be considered merchandise at the border, no matter how broadly that term is defined. Adopting a hybrid approach to electronic devices protects the privacy interests of travelers in wholly unique data; those novel digital effects for which their substantive search has no precedent and little to do with the underlying rationale of the border search doctrine.

[285] *Jones*, 565 U.S. at 415–16; Christopher Pryby, "Forensic Border Searches after *Carpenter* Require Probable Cause and a Warrant," *Michigan Law Review* 118, no. 3 (2019): 523.

[286] Brady, "The Lost 'Effects' of the Fourth Amendment," 955–56.

[287] Brady, 957–58, 1004, 1012. Here, Brady discusses the implications of the *Jones* trespass test.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TIERED, HYBRID-SCOPE-LIMITED ELECTRONIC BORDER SEARCHES

In the context of electronic border searches, a hybrid view of electronic devices paves the way for a scope-limited search protocol in keeping with precedents. The hybrid view calls for suspicion-less electronic border searches to be limited in scope to the core government interests, recognized in *Kolsuz* and *Aigbekaen*, underpinning the existence the border search doctrine itself. Specifically, scope-limited rules authorize recognize the government's authority to search property but limit the depth and breadth of that search to government's need to conduct that search. Such rules ensure that legitimate government interests are protected without personal privacy being eviscerated. Importantly, some scope-limited protocols allow for the scope of a search to be expanded when supported by greater suspicion or government need. In applying search scope-limitations based on the hybrid model, limits on suspicion-less electronic border searches are imposed. This hybrid-scope-limited approach or framework, as it is termed in this thesis, thus ensures the continued constitutionality of border searches of electronic devices undertaken without suspicion. This approach also incorporates a second tier of electronic border search where the scope and manner of such a search can be expanded but only when triggered by an elevated degree of suspicion. The result is a reasonable rule for electronic border searches centered on a tiered, hybrid-scope-limited approach akin, but not identical, to that articulated in *Kolsuz* and *Aigbekaen*.

This chapter first explores other areas of Fourth Amendment law where scope-limited approaches have been adopted to strike a desired balance between significant government interests and personal privacy. An outline of the tiered, hybrid-scope-limited framework for electronic border searches follows. Specifically, a two-tiered concept based on degrees of suspicion is discussed. An examination of the reasonableness of forensic electronic border searches when customs officers possess greater suspicion then follows. The chapter closes with an argument as to why the reasonable suspicion standard in the context of the tiered, hybrid-scope-limited protocol should follow the constitutionally accepted *Terry* definition of that term.

A. OTHER SCOPE-LIMITED APPROACHES TO GOVERNMENT SEARCHES

Scope-limited approaches are not new in the Fourth Amendment context. They allow for varying levels of government intrusion into private property in the event of an overriding government necessity.[288] In such cases the, government intrusions are reasonable so long as the government tailors its conduct to match the rationale that initially justified the intrusion. This tailoring establishes a sliding scale for determining reasonable government conduct that expands in keeping with increased justification.

1. Scope-Limitations in Searches of Vehicles

Carroll not only articulated a hybrid approach designed to stake out a middle ground between the competing interests of the individual and state in the property of motor vehicles, but the case also set forth a scope-limited rule for effecting the desired balance of those interests. Specifically, the rule limits the breadth and degree of a government search, even with probable cause.[289] Only those areas may be lawfully searched where the object that the government is seeking may reasonably be located in the vehicle.[290] In other words, although a law enforcement officer might reasonably search a vehicle's trunk and passenger compartment for a shotgun as evidence of a crime, the scope of that reasonable search may not necessarily extend to the glove-compartment, the engine block or the gas tank.

Searches of vehicles incident to arrest (SIA-V) under *Gant* similarly adapt traditional rules embodying a scope-limited approach in two ways.[291] First, the scope of an SIA-V applies only to areas of the vehicle actually and immediately accessible to an

[288] See Wyoming v. Houghton, 526 U.S. 295, 300–307 (1999).

[289] *Houghton*, at 302.

[290] *Houghton*, at 307. See also *Ross*, 456 U.S. 798.

[291] *Gant*'s two-fold rule provides further instruction through its tiered construct that includes a threshold standard for increasing the scope of an SIA-V tied to an enhanced level of suspicion. See *Gant*, 556 U.S. at 351. As discussed later in this chapter, tethering search scope increases to increased levels of suspicion has direct application for electronic border searches in the context of forensically enhanced searches.

arrested occupant.[292] This restriction exists because the search is meant to safeguard law enforcement and protect against the destruction of evidence.[293] Thus, the extent and depth of an SIA-V under this rationale depends entirely on facts peculiar to the arrest.[294] The second aspect of the *Gant* rule limits a search with probable cause to the crime for which the vehicle's occupant was arrested.[295] For example, if a suspect in a vehicle occupant is arrested for armed robbery, *Gant* permits a search of the vehicle for the evidence of the robbery only with probable cause to believe that such evidence is actually present in the vehicle. This restriction affords the government the ability to recover important evidence supporting the guilt of the occupant before the evidence can be moved or lost. But it precludes law enforcement from rummaging through a vehicle—a person's private property—to develop evidence of new crimes that are, by definition, outside the scope of the search.

2. Protective Search Activity: Frisks and Sweeps

Scope-limited approaches have also been adopted to accommodate the dueling interests of personal liberty and law enforcement officer safety arising from public investigative encounters. For example, protective frisks, under *Terry*, can be undertaken after a law enforcement officer has briefly detained an individual and reasonably suspects, based upon articulable facts, that the person is armed and dangerous.[296] Such frisks protect law enforcement officers from threats to their safety posed by highly concealable weapons.[297] Even the manner is restricted to support the desired scope-limitation, for example, a pat down only with the open palm without a manipulation of objects using the fingers. In this

---

[292] *Gant*, 556 U.S. at 351.

[293] *Gant*, at 335.

[294] For example, if an occupant of a vehicle is arrested while still inside the vehicle, a search of the passenger compartment accessible to that occupant would be reasonable. If the occupant is taken into custody after exiting the vehicle and is handcuffed and placed in a law enforcement vehicle, then a search of the passenger compartment of the vehicle that was carrying the occupant would be unreasonable.

[295] *Gant*, 556 U.S. at 351.

[296] Articulable suspicion is more than a non-specific hunch. In the context of a *Terry* frisk, the term can be defined objectively: particular facts and circumstances known to a law enforcement officer that would cause another officer with similar experience and training to reasonably suspect an individual was armed and dangerous. See *Terry*, 392 U.S. 1.

[297] Minnesota v. Dickerson, 508 U.S. 366 (1993).

way, the law surrounding frisks contains a search scope-limitation. One that attempts to stake out a middle ground measured to protect officer safety while protecting the person frisked from embarrassment or undue impingement on personal liberty.[298]

A scope-limited approach has also been carved from standing Fourth Amendment rules for situations when police are lawfully present in a residence but without a search warrant. Any government search of a home without a warrant has long been viewed under the Constitution, by the judiciary, with wariness.[299] But even in instances when personal privacy considerations are at their peak, rules have been tailored to protect competing government interests—like the need to protect the safety of law enforcement officials. In *Maryland v. Buie*, the Supreme Court adopted a scope-limited rule allowing a non-evidentiary search of a residence incident to a domiciliary arrest.[300] This type of search is referred to as a protective sweep.[301] It is a warrantless search of portions of a residence immediately adjacent to the location of arrest for threats to officer safety.[302] For example, law enforcement officers arresting a subject in a kitchen of a residence may search an adjacent first floor living room but not necessarily an upstairs bedroom. Protective sweeps are limited both in depth—how far law enforcement officers may intrude into a residence—and in breadth—that is, the areas intruded must be capable of concealing a threat.[303]

Significantly, the *Buie* rule, like the rule for SIA-V's, contains a mechanism for the scope of a protective sweep to broaden. That mechanism is tied to a reasonable suspicion that another person, located elsewhere in the residence, poses a risk to law enforcement.[304] Amid such suspicion, law enforcement may increase the scope of a protective sweep,

---

[298] Notably, the scope of a protective frisk expands to open and unlocked containers within a person's possession. See Lee, "Package Bombs, Footlockers, and Laptops," 1447–50.

[299] See Kyllo v. United States, 533 U.S. 27 (2001); Clancy, *The Fourth Amendment*, 167–68; Nelson Lasson, *The History and Development of the Fourth Amendment to the United States Constitution* (Baltimore: Johns Hopkins Press, 1937); and Joseph J. Stengel, "The Background of the Fourth Amendment to the Constitution of the United States," *University of Richmond Law Review* 3, no. 2 (1969).

[300] Maryland v. Buie, 494 U.S. 325 (1990).

[301] *Buie*, at 327.

[302] *Buie*, at 334.

[303] *Buie*, at 334.

[304] *Buie*. at 334–36.

specifically its depth, to all areas of a residence, including those not immediately adjacent to the location of arrest.[305] For instance, in arresting a suspect in a residential kitchen, with reasonable suspicion, a lawful sweep can extend beyond just an adjacent living room into upstairs rooms and any place in a residence where a person may be concealed. In other words, with greater suspicion, the greater weight government interests have, the more reasonable the scope of the warrantless intrusion.

B. DEFINING THE TIERED FRAMEWORK

A hybrid-scope-limited framework for electronic border searches links the scope of electronic device searches to the broad, historically accepted rationale behind the border search doctrine. Under this frame, the examination of electronic devices at the border in their most basic form; i.e., manual (user interface) searches, is related to the following concerns:

- national security,
- the collection of duty and regulation of trade,
- preventing the introduction of harmful goods, and
- regulating immigration to prevent the entry of illegal, inadmissible, or unwanted persons.

Although these concerns authorize broad, suspicion-less customs searches of electronic data they do *not* authorize limitless searches. This scope-limited rule truncates suspicion-less electronic border searches to data—consistent with the hybrid view—that is comparable to physical, tangible property or that may contain information affecting elemental government concerns. This scope-limitation thus extends established border principles originally developed for traditional property to modern electronic devices while still respecting their hybrid nature. Thus, while digital photographs and electronic messages are susceptible to suspicion-less search, a digital effect like health monitoring data is not.

[305] *Buie*, at 334.

1. The Two-Tier Concept

The hybrid-scope-limited approach for electronic border searches incorporates a tiered approach. These tiers, as first espoused in *Cotterman* and developed post-*Riley* in *Kolsuz*, act as a mechanism for increasing the scope of an electronic border search when—as with the *Buie* rule for protective sweeps—increased suspicion is present. In this frame, the first tier of electronic border searches encompasses scope-limited, manual (user interface) searches. Here, customs officers can search data and electronic communications for information related to the four core areas of government concern at the border but cannot search novel digital effects like internet activity or geolocation data.[306] The second tier—when customs officers have reasonable suspicion—allows officials to expand the scope of their search to all data for evidence of criminal activity and to use techniques beyond just manual (user interface) searches. In particular, second-tier, electronic border searches could involve the use of forensic software tools, like those discussed in Chapter II, where every byte of memory on a device is copied and available for search.

This tiered construct follows from the scope escalators tied to enhanced suspicion present in other established warrantless search rationales. The tiered, hybrid-scope-limited framework also remains faithful to existing border search rules that clearly distinguish personal searches from property searches.[307] This framework preserves the long-standing dynamic at the border where government interests are well-established and very powerful.[308] But it also denies the government *carte blanche* permission to employ invasive search methodologies that substantially interfere with a traveler's interests in his electronic devices absent greater suspicion. Only with reasonable suspicion can the government expand searches of electronic devices and enhance their depth and breadth with the aid of forensic tools.

---

[306] U.S. Const., amend. IV.

[307] *Flores-Montano*, 541 U.S. 149.

[308] Clancy, *The Fourth Amendment*, 491–93, discussing the language in border search case law that "speak[s] of that [border search] power in absolutist terms."

2. The Reasonableness of Forensic Electronic Border Searches

Forensic searches of electronic devices use specialized software to make an identical copy of the whole of the data present on a particular device.[309] Among other things, the process reveals data that may have been deleted and that which is opaque to the device's owner during regular use.[310] The original border search statutes discussed the authorities of "customs officers" to act more intrusively when they had "reasons to suspect" criminal activity was present, including violations of customs laws.[311] Forensic border searches are more invasive in their manner and potentially in their scope because, unlike physical, visual examinations of traditional property, they collect more information than the human eye. In the context of *Cotterman*'s luggage analogy, forensic searches parallel searching a piece of luggage for not only the items currently contained therein but for anything that had ever been carried within the luggage.[312] They can uncover data that has been deleted as well as items of metadata which provides for increased granularity in a customs search. They also frequently involve the temporary deprivation a device from its owner. But, in the context of a tiered, hybrid-scope-limited framework, such search is only permissible when customs officers' have reasonable suspicion of criminal activity—in other words cause. The requirement for reasonable suspicion to conduct forensic electronic border searches is reasonable at the border as it is consistent with the legislative history of the doctrine that authorizes customs officers to act more intrusively when armed with greater suspicion.

Ironically, however, forensic electronic border searches are also reasonable given that these searches hold potential benefit for travelers as well. Forensic border searches do involve travelers being deprived of their property. But travelers would experience such a deprivation even if customs officers, armed with reasonable suspicion, only searched electronic devices visually. Given the storage capacity of modern electronic devices, a manual, user-interface searches would be very time consuming. This would necessarily

[309] Kerr, "Searches and Seizures in a Digital World," 541.

[310] Kerr, 542.

[311] Peters, *Public Statutes at Large*, 43.

[312] See *Cotterman*, 709 F.3d at 965.

require that the traveler be deprived of his device for an extended period of time. But, forensic software allows the government to execute its electronic border search off-device.[313] A device would only need to be possessed by customs officers long enough to ensure a bitstream copy of the data had been accurately obtained.[314] The device would then be available for return to the traveler even if the search of the copied data had not yet been completed. In other words, the use of forensic tools to conduct an electronic border search with reasonable suspicion actually could result in a more reasonable intrusion on a traveler's property rights—a shorter property deprivation—than a manual, user-interface search.

Forensic searches, despite the increased intrusiveness of their manner, are reasonable because they can limit the length of time the government searches a traveler's data. Specifically, forensic searches, beyond manual searches, enable customs officers to more quickly and precisely either develop their reasonable suspicion into probable cause or dispel that suspicion all together. They also allow customs officers to conduct targeted searches.[315] For instance, key word searches can be conducted with forensic tools thereby allowing for a more targeted search activity. This can result in only exposing data related to the reasonable suspicion that originally justified the use of more invasive techniques.[316] Nathan Sales has likened forensic key word searches to "dog sniff[s]" of physical property.[317] Only the data that has been alerted to customs officers' attention via the keyword searches need be examined in greater detail.[318] Hence, the reasonableness of forensic electronic border searches is enhanced because a they can preserve a traveler's privacy in other, unrelated data.[319]

[313] Kerr, "Searches and Seizures in a Digital World," 540.

[314] Kerr, 541.

[315] Sales, "Run for the Border," 1119–20.

[316] Sales, 1119–20.

[317] Sales, 1122.

[318] Sales, 1122.

[319] Sales, 1120–24.

Importantly too, forensic searches ensure that only the data carried on a device across the border is subject to search. In this way, a forensic border search could not stray impermissibly into data stored off-device in the "cloud."[320] Finally, a forensic border search provides a snap shot in time of the data contained on an electronic device. Kerr has recognized that searches with forensic tools afford an "evidentiary integrity of the original evidence," that is not possible with manual searches.[321] Thus, the reasonableness of forensic electronic border searches is further established by the fact that in the event of future litigation, travelers and defense attorneys are assured of the exact context in which items of data indicative of criminal activity were found.

3. The Need to Follow *Terry*'s Definition of Reasonable Suspicion

For many reasons, *Terry*'s constitutionally accepted definition of reasonable suspicion, tying it to evidence of criminal activity, is the one that must be followed for electronic border searches in the second tier of the proposed framework. Straying from this definition as courts that have confronted the question of electronic border searches since *Riley* have, leads to illogical results. Any adoption of a novel definition for reasonable suspicion, specifically in the context of border searches of electronic devices, recalls the now discredited attempts by the Ninth Circuit in the 1960s, 1970s, and 1980s to arbitrarily manufacture an entirely new level of suspicion for personally intrusive border searches.[322]

Reasonable suspicion has been established as the highest level of justification necessary for any government border search.[323] At the border, reasonable suspicion allows for intimate breaches of a person's body regardless of the fact that the "integrity of an

[320] Margaret Rouse, "Cloud Storage," SearchStorage, accessed September 18, 2020, https://searchstorage.techtarget.com/definition/cloud-storage.

[321] Kerr, "Searches and Seizures in a Digital World," 540.

[322] See Rivas v. United States, 368 F.2d 703 (9th Cir. 1966); United States v. Castle, 409 F.2d 1347 (9th Cir. 1969); United States v. Summerfield, 421 F.2d 684 (9th Cir. 1970); United States v. Sosa, 469 F.2d 271, 272 (9th Cir. 1972); and United States v. Shields, 453 F.2d 1235 (9th Cir 1972). These cases articulated a novel standard of suspicion referred to as the "clear indication" or "plain suggestion" standard that was inserted as a level of suspicion between reasonable suspicion and probable cause. This string of case law was struck down by the Supreme Court in 1985 in *Montoya de Hernandez.*

[323] *Montoya de Hernandez*, 473 U.S. at 540–42.

individual's person is a cherished value in [American] society."[324] But a novel definition of reasonable suspicion for electronic border searches would create a huge imbalance in which the government has the authority to grossly invade a traveler's body but not his electronic device. For instance, a restrictive definition of reasonable suspicion, like one limiting that suspicion to the presence of child pornography, would create declare significant invasions of a person's body to recover any item, including an electronic device, acceptable, but not a search of the data present on a recovered device. Courts have logically found that subjecting individuals to the indignities of revealing their bodies and probing their orifices represent more severe invasions of privacy than that involved in the search of property, even when the property is electronic in nature.[325] A special definition of reasonable suspicion narrower than *Terry*, however, violates this logic. Such a definition would strangely declare invasive searches of the body as less offensive than searches of digital property.

a. Problems Created by the Kolsuz-Aigbekaen Standard

The *Kolsuz* definition of reasonable suspicion is too restrictive. Its definition, further enshrined in *Aigbekaen*, also goes beyond *Terry*'s long-standing linkage of reasonableness to criminal activity. The *Kolsuz-Aigbekaen* standard imposes a nexus requirement——one that limits reasonable suspicion only to criminal activity of an "ongoing" and "transnational" character.[326] Those courts sought to align second-tier, forensic electronic border searches to material related to the government's broad, historic interests at the border versus "generalized" crime-fighting.[327] However, these courts, in inventing a novel definition of reasonable suspicion relative to the border search of the electronic devices, implicitly composed dueling definitions of reasonable suspicion in the border environment: one rooted in criminal activity for searches of people and traditional property and one that requires a nexus to "ongoing transnational crime" for electronic

[324] *Summerfield*, 421 F.2d at 685, citing Schmerber v. California, 383 U.S. 757 (1966).

[325] See *Montoya de Hernandez*, 473 U.S. 531; and *Touset*, 890 F.3d 1227.

[326] *Kolsuz*, 890 F.3d at 144. See also *Aigbekaen*, 943 F.3d 713.

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

devices only.[328] Accordingly, *Kolsuz* and *Aigbekaen* establish a two-track definition of reasonable suspicion at the border that again promotes form over substance. A customs officer can conduct invasive, physical searches of people or destructive searches of property with reasonable suspicion of criminal activity but can only forensically search electronic devices with reasonable suspicion when that suspicion is tied to crimes that are transnational in nature. It is an inconsistency not readily explainable when "the object of the search" and not what is being searched is what is important.[329] Such a definition of reasonable suspicion threatens doctrinal consistency in property searches at the border and sets a dangerous precedent potentially opening the door for the creation of multiple categorical border search rules.

Kolsuz's and *Aigbekaen*'s definition of reasonable suspicion is also problematic because it ignores the statutory standing of customs officers. All customs officers who police the borders are also sworn federal law enforcement officers authorized to enforce customs statutes and other federal criminal statutes.[330] For instance, HSI Special Agents, are customs officers who are also responsible for the enforcement of more than 400 statutes of the United States criminal code.[331] Their investigative and enforcement authority is rooted in Title 19—the Customs title—among other statutes.[332] The *Kolsuz-Aigbekaen* standard would require courts to speculate as to which crimes fall under the broad umbrella of customs officers' authority and which do not. This standard could quickly become murky in an era in which evolving technology, trade, travel, and finance blurs any bright line seeking to separate wholly internal criminal activity from that which has some cross-border character.

---

[328] The *Kolsuz* decision left the application of the reasonable suspicion standard, as defined by *Terry*, to invasive personal or destructive property searches intact.

[329] *Ross*, 456 U.S. at 824.

[330] Katelin P. Isaacs, *Retirement Benefits for Federal Law Enforcement Personnel*, CRS Report No. R42631 (Washington DC: Congressional Research Service, 2017), 3.

[331] "The Life Saving Missions of ICE," Department of Homeland Security, August 20, 2018, https://www.dhs.gov/news/2018/08/20/life-saving-missions-ice.

[332] 19 U.S.C. § 1589a (2008).

In addition, the *Kolsuz-Aigbekaen* reasonable suspicion standard presents other logical dilemmas leading to uncertainty in application. Those courts own pronouncements about tethering reasonable suspicion to the established purposes of the border search doctrine and that forensic electronic border searches are reasonable so long as they are related to "ongoing transnational crime" conflict with one another.[333] For instance, consider a customs broker working alone and falsifying declarations for merchandise that has already been imported. A forensic electronic border search of digital devices belonging to the customs broker for evidence related to his fraud would certainly be included under the rationale for the existence of broad customs search authority. Despite the fact that the goods mentioned on the fraudulent paperwork may have traveled internationally, the customs broker's fraud is wholly domestic. Under the *Kolsuz-Aigbekaen* view of reasonable suspicion, it may be that the international nexus; i.e., the goods crossing the border, is not strong enough to support a lawful border search.[334] Consider as well the potential nexus of a money launderer based in the United States. His illegal actions may not implicate questions related to customs interests as they have been defined but may have "ongoing" and "transnational" components.[335] This situation could happen if the money launderer uses virtual currencies or electronic communications to perpetrate his crimes that reside on or pass through internationally based servers. Whether this situation would constitute a sufficient international nexus under the *Kolsuz-Aigbekaen* frame to justify a forensic border search remains unknown.

Additional problems with the *Kolsuz-Aigbekaen* nexus test can be seen in considering other criminal activity with potential international components. Consider a domestic homicide committed by a member of the gang MS-13. *Kolsuz* and *Aigbekaen* would certainly characterize an electronic border search of a homicide suspect as being of a "generalized" investigatory nature and would see any reasonable suspicion of a homicide

[333] *Kolsuz*, 890 F.3d at 144.

[334] See *Aigbekaen*, 943 F.3d at 730–34 (Richardson, J., concurring) for the pitfalls of the *Aigbekaen* majority's "nexus test."

[335] *Kolsuz*, 890 F.3d at 144.

as unconnected to the border search doctrine's purpose.[336] But gangs like MS-13 and others do operate internationally.[337] At higher levels, domestic gang leaders and foreign-based members communicate.[338] So while the homicide suspect may not have such contact, his parent gang may. And in that case, would the electronic border search then not be reasonably related to "ongoing transnational crime?"[339] Finally, consider the application of the *Kolsuz* reasonable suspicion standard to street level cocaine distribution. Such conduct may not be transnational but when viewed through the understanding that cocaine is not manufactured in the United States but rather flows across the national boundaries, such activity does have a nexus to the border and relates to customs interests.[340] These scenarios bring into sharp relief the logical problems and application hurdles of the *Kolsuz-Aigbekaen* reasonable suspicion standard. Moreover, they ignore what one jurist from the *Kolsuz-Aigbekaen* Circuit has recognized: "The purposes of the border-search doctrine overlap to some degree with general law enforcement."[341]

Notably, the *Aigbekaen* court confronted the problems created by the nexus test and failed to logically apply it. That failure occurred when that court left unaddressed an important fact which should have upended its analysis. In finding an electronic border search of a suspect involved in domestic sex trafficking as unreasonable because the reasonable suspicion did not relate to "ongoing transnational" criminal activity, the court did acknowledge that the main suspect was Nigerian.[342] Though the court did not specify the suspect's immigration status, the opinion did tacitly acknowledge that the individual was not a U.S. national as the term is defined in law.[343] This status meant the suspect was

---

[336] *Kolsuz*, at 143.

[337] Center for Latin American and Latino Studies, *MS13 in the Americas: How the World's Most Notorious Gang Defies Logic, Resists Destruction* (Washington, DC: American University, 2018), https://www.justice.gov/eoir/page/file/1043576/download.

[338] Center for Latin American and Latino Studies, 60.

[339] *Kolsuz*, 890 F.3d at 144.

[340] Eric Goldschein, "Following the Cocaine Trail: How the White Powder Gets into American Hands," Business Insider, December 8, 2011, https://www.businessinsider.com/cocaine-facts-2011-12.

[341] *Aigbekaen*, 943 F.3d at 730–31 (Richardson, J., concurring).

[342] *Aigbekaen*, at 717.

[343] 8 U.S.C. § 1101(a)(21) (2011).

a foreign national subject to a range of U.S. immigration laws. Depending then on the extent and the nature of his misconduct, the suspect may have been inadmissible or otherwise subject to removal proceedings under those laws.[344] According to *Aigbekaen*'s own rationale, following that of *Kolsuz*, enforcing immigration laws and preventing undesirable persons from entering the country falls square within the border search mandate.[345] Following the lessons of *Kolsuz* then, the court should have endorsed, not nullified, the reasonableness of the border search.[346] The *Aigbekaen* court, however, in attempting to follow in *Kolsuz*'s footsteps and substantiate a novel reasonable suspicion standard failed to logically apply that standard.

b. Clarity via the Terry Standard

Importantly, even those who are critical of electronic border searches and who have argued for implementation of a reasonable suspicion standard for some electronic border searches ascribe to the *Terry* definition.[347] Tethering reasonable suspicion to "criminal activity" still affords the protection of privacy in electronic data desired by *Kolsuz* but eliminates its logical inconsistencies.[348] Whereas the *Kolsuz-Aigbekaen* standard may have difficulty assessing the reasonableness of a forensic border search of a suspected terrorist, one who while posing a national security threat, may not include a threat of an "ongoing" or "transnational" character, the *Terry* standard makes no such distinction.[349] Adherence to *Kolsuz-Aigbekaen* reasonable suspicion construct allows the electronic devices of a radical Salafist-jihadist to be forensically border searched but demands that devices of a white-supremacist terrorist be excepted. Each one threatens the sovereign's security, but *Kolsuz-Aigbekaen* rule fosters anomalous results.

---

[344] See, generally, 8 U.S.C. § 1182 (2011).

[345] *Aigbekaen*, 943 F.3d at 721.

[346] Noting the petitioner as "a foreign national having traveled from abroad into the United States with the intent to continue his criminal activity," Richardson, citing United States v. Oriakhi, 57 F.3d 1290, 1296 (4th Cir. 1995), discusses the purpose of the border search doctrine and "the sovereign's power to protect itself . . . to exclude harmful influences, including undesirable aliens, from the sovereign's territory." *Aigbekaen*, 943 F.3d at 733–44 (Richardson, J., concurring).

[347] Park, "The Elephant in the Room," 309–12.

[348] Park, 309–12.

[349] *Kolsuz*, 890 F.3d at 144.

Returning to the established *Terry* standard is the best approach for establishing the reasonableness benchmark for second-tier border searches using forensic tools. That standard is consistent and well-established. It avoids creating different definitions for reasonable suspicion in the border environment. It avoids the logical inconsistencies created by more restrictive definitions of that term. *Terry*'s reasonable suspicion definition also eliminates the problems and uncertainty created by the *Kolsuz-Aigbekaen* definition. It does not require nuanced assessments as to whether illegal activity is of a sufficient transnational character to authorize searches of increased scope and manner. By linking reasonable suspicion to the presence of criminal activity, customs officers can be clear and certain as to when second-tier, forensic electronic border searches may be conducted.

C. CONCLUSION

The tiered, hybrid-scope-limited approach to electronic border searches addresses concerns centered on their potentially boundless nature. It also mitigates concerns as to the manner in which electronic border searches are conducted. The framework's tiered construct provides for a measured approach requiring greater intrusions to have greater justification. The tiered, hybrid-scope-limited model achieves this not through haphazard rule-making but through the tailoring of long-recognized principles. In addition to limiting the scope of suspicion-less searches, it also limits their manner. It also, however, allows for electronic border searches to expand with increased justification. This model sanctions the use of forensic tools and an increased search scope, beyond the elemental interests the government has for conducting searches of property at the border, when reasonable suspicion is present. In particular, when customs officers are armed with increased suspicion, forensic electronic border searches, though seemingly more invasive, are a reasonable search modality. Finally, the reasonable suspicion requirement for second-tier electronic border searches in this electronic border search framework must adhere to *Terry*'s definition in order to avoid anomalous and illogical results.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION: GUIDANCE FOR PRACTITIONERS

Adopting a tiered, hybrid-scope-limited framework in an electronic border search policy could guide customs officers in their exercise of this unique authority. It could assist customs officers in properly scoping their suspicion-less, user-interface searches in the first tier. It could also provide how the manner of their search can expand, using forensic tools, in the second tier, when the officer has reasonable suspicion. Although CBP updated its electronic border search policy in 2018, ICE-HSI's new policy is still under revision in light of issues raised by courts in the post-*Riley* era.[350] Any customs agency interested in developing, reviewing, or amending its policy regarding electronic devices encountered at the border can benefit from an articulation of a tiered, hybrid-scope-limited framework. Such a policy provides a baseline on which customs officers can conduct their searches of electronic devices. It also fosters uniformity by eliminating vagaries in practice, thereby, making the overall execution of electronic border searches more reasonable. In addition, a policy instituting the tiered, hybrid-scope-limited approach promotes perceptions of reasonableness by aligning with other legally accepted precedents.

This final chapter examines how the tiered, hybrid-scope-limited framework maintains the historic balance between the power of the government and individual privacy rights at the border. An answer to the first research question—whether or not electronic border searches after *Riley* continue to be constitutionally acceptable—follows. Next, this chapter answers the other question: how can the constitutional reasonableness of electronic border searches be maintained in the long term? It discusses how the tiered, hybrid-scope-limited approach for electronic border searches can guide customs officers in the exercise of their authority and how existing rules can be translated to address novel issues presented by modern technology. This chapter concludes by looking at why electronic border searches conducted in accordance with the tiered, hybrid-scope-limited model represent a reasonable and necessary resolution to the electronic border search debate that has grown since the *Riley* decision.

[350] See Customs and Border Protection, *Border Searches of Electronic Devices.*

A. TIERED, HYBRID-SCOPE-LIMITED APPROACH: MAINTAINING THE BORDER BALANCE

The tiered, hybrid-scope-limited rule for electronic border searches preserves the historic, purposefully established tension between the competing interests of government in promoting safety, security, and the popular welfare versus the privacy rights of the individual. Importantly, the rule seeks balance not equality. The balance to be struck at the border leans heavily in favor of the government and customs searches are meant to be of "broadest possible character."[351] The depth and character of reasonable government searches at the border can be extreme, like those involving a person's body cavities.[352] Similar searches in the interior would be excessive. Thus, the border search doctrine's purpose is to allow for searches that while unreasonable in the interior are reasonable at the border.[353]

Likewise, unlike in the interior, encounters between people and government officials are not consensual but obligatory. People must provide information to the government concerning private details about their travel, currency, and items they seek to bring into the country. Failures or inaccuracies subject one to the potential of criminal penalties.[354] So different is the legal paradigm of the border that at one point Congress required individuals with a history of drug offenses to register with and self-declare to customs officers upon seeking to enter or exit the United States.[355] The imposition of such affirmative requirements on travelers to present themselves and their property for inspection when crossing the border demonstrates the obvious weight of government authority to preserve the safety and security of nation at the expense of personal liberty.

---

[351] United States v. Yee Ngee How, 105 F. Supp. 517, 520 (N.D. Cal. 1957).

[352] Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment*, vol. 5, 5th ed. (St. Paul, MI: West, 2012): 252–53. See also Ittig, "Rites of Passage."

[353] Peters, *Public Statutes at Large*, 43.

[354] 19 U.S.C. § 1592 (2010); 13 U.S.C. § 305 (2018).

[355] *Rivas*, 368 F.2d at 703, citing 18 U.S.C. § 1407, "Border Crossings—narcotics addicts and violators," enacted July 18, 1956, as part of the Narcotics Control Act of 1956, and repealed October 27, 1970.

Any artificial limitations of manual electronic border searches based on *Riley*'s rationale are also misguided. If the border balance aims for the sovereign to protect itself through "plenary customs power," then the rules delineated in *Cano* and *Alasaad* are not viable.[356] Limiting manual electronic border searches only to situations where reasonable suspicion of contraband exists is far too restrictive.[357] Preventing a border search from seeking out data beyond that which only involves child pornography is both unreasonable and unsupported in law. Rationale for the border search doctrine has never been limited to simply discovering contraband.[358] Such a rule is inconsistent with the purpose underlying the border search doctrine, which is sovereign protection.

But another artificial rule, one that limits manual electronic border searches only to determine whether data is present on a device, is more dangerous still.[359] Such a rule would destroy the long-established border equilibrium effectively rendering the border search doctrine impotent. It would grant perfect protection to national, customs, and immigration threats based merely on their form in binary code. Extending the rationale of one court to the potentiality of such a rule begs the question: if digital devices and data are "to be left unwatched," what is the purpose of subjecting all persons and physical goods to border searches, no matter how intrusive the manner or how private the item?[360] This rule would reduce the government's ability to protect the nation at the borders based on form alone. Rather than crafting new rules that disturb the purposefully established balance between the government and the individual at the border, the tiered, hybrid-scope-limited approach transfers the desired balance from the realm of physical property to the digital one. The reasonableness of border searches then is not determined by what is being searched but rather by the purpose and scope of the search.

---

[356] *Ramsey*, 431 U.S. at 616.

[357] See *Aigbekaen*, 943 F.3d at 730 (Richardson, J., concurring): "This 'contraband-only' view might be too narrow given the interests of the United States, as sovereign, at its territorial borders."

[358] See *Ramsey*, 431 U.S. 606.

[359] See *Alasaad*, No. 17-cv-11730-DJC.

[360] Cotzhausen v. Nazro, 107 U.S. 215, 218 (1883).

B. CONSTITUTIONALITY OF ELECTRONIC BORDER SEARCHES AFTER *RILEY*

Though *Riley* shifted the Fourth Amendment dynamic for warrantless searches of electronic devices in the interior, at the border, such searches continue to be constitutionally permissible. In the six years since the *Riley* decision, no court has outlawed the electronic border search practice or imposed categorical warrant requirements. Thus, for all of argument over whether *Riley* created a new, special category for electronic devices, courts have continued to find that customs search authority does include the power to search personal electronic devices and data.

Aside from the judiciary's continuing sanction, other reasons explored in this thesis establish *Riley*'s limited impact on electronic border search practice. Chiefly, Congress has "declared that a search which [is] 'unreasonable' . . . if conducted by police officers" within the U.S. is "reasonable if conducted by customs officials" in furtherance of their duties at the border.[361] The government's power to search at the border simply cannot be so "severely impede[d]" that it wholly affects the efficacy of the government efforts to fulfill core interests of sovereignty.[362] Of added significance was the *Riley* Court's decision to choose a case involving the SIA exception to discuss the uniqueness of electronic devices restricts *Riley*'s application. Far from seeking to confine the authority of customs officers, the High Court has admonished lower courts "to interpret the [border search] doctrine broadly and avoid creating new limitations."[363] In this respect, border searches are unique. The border search doctrine is the product of a deliberately constructed two-fold search paradigm: one set of rules for the border and another for the interior. Border searches stand independently from other searches. They have not been carved from but rather exist alongside the Fourth Amendment.

[361] *Rivas*, 368 F.2d 703.

[362] United States v. Guadalupe-Garza, 421 F.2d 876, 879 (9th Cir. 1970).

[363] *Aigbekaen*, 943 F.3d at 730 (Richardson, J., concurring).

C. ENSURING THE REASONABLENESS OF ELECTRONIC BORDER SEARCHES

Finding electronic border searches as constitutionally reasonable post-*Riley*, however, only addresses one of the questions posed by this thesis. The second focuses on ensuring their continued reasonableness moving forward. It is foreseeable that evolving technologies will make the bright-line border search rule allowing robust searches of anything crossing the border, tangible or intangible, increasingly controversial. So, while wholly outlawing electronic border searches is neither desirable nor logical, an enduring solution to maintaining their reasonableness must not gloss over the central role electronic devices and data increasingly play in people's lives. Instead of following a categorical, anything-goes-at-the-border view, electronic border searches should be rooted in the original purposes for the doctrine. By doing so, reasonable limitations can be imposed on the scope and manner of suspicion-less customs searches, thereby ensuring their continued compatibility with the Constitution in the future.

The hybrid-scope-limited approach that this thesis suggests imposes such limits. By treating electronic devices as both containers and novel property in which both the government and the individual have compelling interests, the approach tailors the scope of customs searches in a reasonable way. It preserves the ability of the government to guard against traditional threats now stored or facilitated electronically. Simultaneously though, the approach protects personal privacy by not allowing the government unfettered access to the whole of a person's digital life absent more. The approach also limits the government's interference with a traveler's possessory interests in his electronic devices by limiting the manner in which a suspicion-less electronic border search can be conducted. The addition of a second-tier border search also provides a mechanism to reasonably balance the competing interests of the state and individual at the border; one where the scope and manner of search can be expanded but only with reasonable suspicion of criminal activity.

The tiered, hybrid-scope-limited framework for electronic border searches, thus, not only promotes but provides for the continuing maintenance of the reasonableness of such searches. It creates a flexible electronic border search rule that focuses on the

substance of the data held in electronic devices, not its unique form. This focus allows the rule to translate existing rules to new types of property, making it adaptable as necessary to deal with advances in technology. The tiered nature of the framework affords customs officers greater authority to protect important national interests when greater justification is present. On a macro level, this framework ensures electronic border search's long-term constitutionality while preserving the purposefully established dynamic that offsets personal privacy with uniquely broad government power at the border. At a micro level, the tiered, hybrid-scope-limited frame provides a conceptual basis for customs officers to use in exercising their electronic border search authority. This framework can guide customs officers when confronting ever-evolving forms of property and dealing with the distinctive issues they present.

D. PRACTITIONER'S GUIDANCE: DEALING WITH NOVEL ELECTRONIC BORDER SEARCH ISSUES

Questions over government searches of electronic devices and data are not going away, especially at the border. In 2015 alone, in excess of 382 million travelers crossed the U.S. border at various ports of entry.[364] Given the ubiquity of electronic devices acknowledged by the *Riley* court, one may easily assume that the number of electronic devices that crossed the border in the carriage of these travelers was far greater.[365] Accordingly, border searches where electronic devices are involved will only grow. Therefore, customs officers need to be prepared for the novel issues presented by electronic devices and ensure that their border searches are fairly conducted.

The tiered, hybrid-scope-limited approach can provide conceptual guidance to customs officers in conducting electronic border searches and in confronting issues unique to such searches. These issues include: cloud connectivity, copying and retaining electronic data, and confronting locked and encrypted devices. Guidance for confronting these issues

[364] "CBP Releases Fiscal Year 2015 Trade and Travel Numbers," Customs and Border Protection, March 4, 2016, https://www.cbp.gov/newsroom/national-media-release/cbp-releases-fiscal-year-2015-trade-and-travel-numbers.

[365] *Riley*, 573 U.S. at 385. See also Carpenter v. United States, 138 S. Ct. 2206 (2018), which discusses the prevalence of mobile phones in the United States.

is discussed in the following sections. Notably, the guidance discussed does not consist of a checklist for customs officers to follow. Adherence to a checklist is not a guarantee of reasonableness in every case. For instance, existing policies that are being reconsidered in light of *Kolsuz* and other cases articulate that devices can be detained for 30 days with a 15-day extension granted by a supervisor.[366] But just because a customs officer's detention of electronic devices meets this timeline does not establish his conduct as reasonable on its face. A customs officer may meet this policy requirement if he detained a traveler's electronic devices but waited until day 28 to conduct his border search. The customs officer may very well accomplish his search and return the devices by day 30 but the act of waiting until day 28 to conduct the search could be determined to be unreasonable in that it resulted in a traveler being deprived of his property longer than was necessary. Conversely, there might be extenuating circumstances that increase the time necessary to undertake a border search making such a search far beyond 30 days reasonable. Because Fourth Amendment reasonableness is quite frequently dependent on the particular facts surrounding a search, a universal checklist is of limited value. Instead, conceptual guidance provides a frame for the discretionary decision-making of customs officers when dealing with searches of electronic devices and the unique issues they present. Such guidance also instructs customs officers as to how to articulate the reasonableness of their conduct.

1. "Cloud" Connected Devices and Programs

Under a tiered, hybrid-scope-limited framework, electronic border searches must continue to be limited to only that which has been downloaded to a device by the user prior to crossing the border. Any data not within the physical memory of such a device as it transits the border cannot reasonably fall within the scope of a proper electronic border search. This limitation is important because today's electronic devices can access information both stored on the device and stored elsewhere. A device can do this by accessing different data sites via the internet or by accessing the user's data stored, not on the device, but on remote, disparate servers. The latter is "cloud" data, to which a user has

[366] Immigration and Customs Enforcement, *Border Searches of Electronic Devices*.

ready and immediate access.[367] A traveler can access such data either by linking his electronic device to such storage or through the use of cloud-based applications and programs.[368] Data stored in the "cloud," however, is not data stored or contained within an electronic device itself.[369] This type of data gave the *Riley* court pause in the context of searches of electronic devices incident to arrest.

Critics, too, have expressed concerns that electronic border searches are unreasonable because they could stray into off-device, cloud data, including data that reveals intimate information of one's home.[370] But, in order to view this data, network connectivity for the device is required. To achieve this physical scope-limitation, customs officers can isolate electronic devices from wireless and cellular networks, utilizing device "airplane modes," before initiating any border search.[371] Such action prevents any data transmission to and from a device. Thus, data stored remotely would be inaccessible. Personal information held and accessed via cloud-based applications on a traveler's electronic device would be physically beyond the reach of a search at the border as well. Without a network connection, both the customs officer and the traveler can be confident that the only information subject to search is that which is present within the physical memory of the device. Then, only data that physically crossed the border is available for examination.

2. Data Copying and Retention

Electronic border searches conducted within the tiered, hybrid-scope-limited framework do allow customs offices to copy a traveler's data with reasonable suspicion, and retain that data with cause to believe that the data contains evidence of a crime. To

[367] Rouse, "Cloud Storage."

[368] Zach Barton, "What Is a Cloud Application?," *CloudBakers* (blog), April 18, 2018, https://www.cloudbakers.com/blog/what-is-a-cloud-application.

[369] Rouse, "Cloud Storage."

[370] See Donohue, "Customs, Immigration, and Rights."

[371] Philip Bates, "What Is Airplane Mode on IPhone? Everything You Need to Know," MakeUseOf, June 22, 2020, https://www.makeuseof.com/tag/everything-need-know-airplane-mode-iphone-ipad/. The policy specifically directs CBP officers to ensure all inspected devices are unconnected to networks or otherwise placed in airplane mode.

date, fears related to the copying and retention of a traveler's private data have fueled concerns as to the unreasonableness of electronic border searches.[372] Some fear that such a practice portends the creation of a government surveillance state while others fear that their privacy may be permanently compromised as travelers' lose possession and control over the dissemination of their data.[373] Customs officers, however, are permitted to make copies of documents and other information in the "paper world."[374] For example, customs officers can copy and retain physical property, including documents, if translation is required or if assistance from outside experts is necessary to determine whether the contents relate to violations of customs laws.[375] In addition, the federal rules of criminal procedure authorize the copying of data from electronic devices for the purpose of facilitating a law enforcement search.[376] Within the United States, the government's copying of data pursuant to searches of electronic devices is judged only by what is reasonable.[377] That reasonableness hinges only on what is the government's rationale for copying of data. Thus, these federal rules recognize that "as long as the government has a law enforcement purpose in copying records, there is no reason why it should be saddled with a heavy burden of justifying" such action.[378]

---

[372] "Border Agents Are Copying Travelers' Data, Leaving It on USB Drives," *Naked Security* (blog), December 13, 2018, https://nakedsecurity.sophos.com/2018/12/13/border-agents-are-copying-travelers-data-leaving-it-on-usb-drives/.

[373] See, generally, Kerr, "Searches and Seizures in a Digital World," 569; and Kerr, "Fourth Amendment Seizures of Computer Data,"703–5.

[374] Robles, *Law Course*, 179, discusses the authority to copy documents at the border with reasonable suspicion. See Fed. R. Civ. P. 41, Committee Notes on Rules–2009 Amendment (seeking to maintain the protocols for copying and searching computer data as consistent with the copying and searching of paper documents).

[375] Robles, *Law Course*, 179.

[376] H. Marshall Jarrett et al., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Washington, DC: Department of Justice, 2009), 76–78; Fed. R. Civ. P. 41, Committee Notes on Rules–2009 Amendment ("acknowledg[ing] the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls with the scope of [what may be seized]").

[377] "The fourth amendment protects people from unreasonable seizures . . . and reasonableness under all of the circumstances must be the test when a person seeks to obtain the return of property. . . . If the United States' legitimate interests can be satisfied even if the property is returned, continued retention of the property would become unreasonable." Fed. R. Civ. P. 41, Committee Notes on Rules–2009 Amendment.

[378] Fed. R. Civ. P. 41, Notes of Advisory Committee on Rules–1989 Amendment.

Within the second tier of the proposed framework, once reasonable suspicion of criminal activity has been developed, a forensic border search in which a traveler's data is copied, may be conducted. Here, constitutional reasonableness is satisfied because once armed with reasonable suspicion, customs officers have a legitimate interest in copying the data. Data copying affords customs officers the ability to detain a traveler's data in its original form in order to facilitate a further, in depth review—the goal of which is to resolve that suspicion. This copying and limited retention of data is akin to an "investigative detention" under *Terry*.[379] Accordingly, the copying and retention would fulfill the narrow purpose of allowing customs officers to conduct a review to determine whether items within the data are evidence of crime thereby establishing probable cause. As with *Terry*, this "investigative detention" of the information cannot be unduly long.[380] Rather, in copying and retaining data for this purpose, customs officers must demonstrate due diligence in reviewing the data to either confirm or dispel suspicions.[381] If items of data afford probable cause of criminal activity, the data, just as it would under Federal Rules of Criminal Procedure Rule 41, can be seized and preserved; i.e., retained, as evidence.[382] If probable cause is not developed, the data must be destroyed.

In addition, documentation capturing the copying and retention or destruction of data obtained under electronic border searches is important. Justice Breyer has noted the importance of record-keeping as an element of reasonableness in the conduct of border searches.[383] With defined reporting requirements as part of a tiered, hybrid-scope-limited electronic border search policy, ad hoc practices like when customs officers conduct

[379] Steven L. Argiriou, "*Terry* Stop Update: The Law, Field Examples and Analysis," Federal Law Enforcement Training Centers, accessed September 23, 2020, https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/4th-amendment/terrystopupdate.pdf.

[380] According to Argiriou, "A . . . [detention] in connection with a *Terry* stop [can only be] for as long a period as is reasonable." Argiriou, "*Terry* Stop Update," 5.

[381] *Terry*, 392 U.S. at 28, 30; Argiriou, "*Terry* Stop Update."

[382] See Fed. R. Crim. P. 16(a)(1)(E) (requiring the government, as part of its discovery obligations in a criminal prosecution to "permit the defendant to inspect and to copy . . . data" when "the item was obtained from or belongs to the defendant"). Consequently, the retention of copied data subsequently seized pursuant to a forensic border search is mandatory for the government to meet its discovery obligations.

[383] *Flores-Montano*, 541 U.S. at 156–57 (Breyer, J., concurring).

electronic border searches by downloading personal data on to thumb-drives without any chain of custody can be prevented.[384] Specifically, when data copied from devices detained at the border are devoid of criminal evidence, customs officers operating within the second tier of the proposed framework, should document their negative findings and ensure any data that have been copied are erased. If information reviewed does reveal evidence of crime, documentation recording the seizure and retention of that data as evidence should be accomplished. Such a protocol adheres to accepted electronic device search methodologies for the copying and retention of data and, when coupled with appropriate documentation, establishes, on its face, the reasonableness of customs officers' conduct when conducting second-tier electronic border searches.

3. Locked Devices and Encryption

In exercising their border search authority over electronic devices in a tiered, hybrid-scope-limited scheme, customs officers have the authority to demand that electronic devices be unlocked and decrypted in order to allow for examination of their digital contents. The design of modern electronic devices which enable them to be locked, password protected, and their data encrypted present challenges to customs officers' authority. But compliance with customs officers at the border is not a choice, and border searches are not consensual.[385] Customs officers can exercise "all necessary force" to "compel compliance" in the conduct of their border search authority.[386] So it stands then that the government is not impotent when confronted with locked or encrypted electronic device at the border. The government's authority for dealing with such situations is constitutionally implicit and sanctioned under the concept of implied powers. It is axiomatic that "clearly established in law or in reason . . . that wherever the end is required, the means are authorized."[387] Put another way, "wherever a general power to do a thing is

[384] "Border Agents Are Copying Travelers' Data."

[385] 19 U.S.C. § 1582; 19 U.S.C. § 482.

[386] 19 U.S.C. § 1581.

[387] James Madison, *The Federalist* No. 44, quoted in Sheldon Richman, "TGIF: James Madison: Father of the Implied-Powers Doctrine," Future of Freedom Foundation, accessed September 5, 2020, https://www.fff.org/explore-freedom/article/tgif-james-madison-father-of-the-implied-powers-doctrine/.

given, every particular power necessary for doing it is included."[388] Therefore, because the government has a general power to conduct border searches of persons and property, which include electronic devices, it can reasonably exercise the necessary power to effect its search and overcome obstacles presented by technology.

Moreover, border search statutes already contemplate encounters with locked containers. Here the government's authority at the border is legislatively explicit. Customs officers have long had the power to "demand" keys from any traveler to examine a locked container.[389] In instances when a traveler refuses to unlock a container or provide a key in order to facilitate a border examination, a customs officer has recourse.[390] Congress has stated that, under these circumstances, customs officers "shall" detain the locked container for the purposes of gaining access to its contents and undertaking a border examination.[391] Under a hybrid view of electronic devices, the same rationale would apply to locked electronic devices and encrypted data. If information that affects the broad scope of the government's authority at the border is to be subject to inspection, then the locking of devices or the presence of encryption should not defeat the exercise of border search authority. Just as a traveler cannot avoid a customs examination of the contents of his briefcase merely by refusing to provide its combination, a traveler cannot sidestep a search of his electronics merely by refusing to provide his passwords.

Constitutional principles of reasonableness and implied powers afford customs officers the ability to demand decryption passwords to view pertinent information stored on a device. If a traveler refuses to comply, customs officers can reasonably hold a device up to a traveler's face or demand their finger prints to accomplish unlocking and decryption. If a traveler continues to resist and the physical unlocking measures described are unavailable to the customs officers, or cannot be reasonably undertaken, the device can be detained. The detention is not punitive. It also does not require any particular suspicion. Rather the purpose of the detention is simply to afford customs officers additional time to

[388] Madison, *The Federalist* No. 44.

[389] 19 U.S.C. § 1461 (2018).

[390] 19 U.S.C. § 1462 (2018).

[391] 19 U.S.C. § 1462.

make efforts to overcome locked devices and encryption and execute a suspicion-less, hybrid-scope-limited, border search. This contingency is both reasonable and legislatively sanctioned in the border environment.[392]

Unlocking electronic devices has been addressed by at least one court of review concerning electronic border searches. In *Wanjiku*, the Seventh Circuit dealt with the question of password protection and encryption. In seeking to conduct a border search of a traveler's cellular phone, customs officers demanded the password to unlock the device.[393] The traveler was initially reticent.[394] Customs officers then explained the device would be removed from traveler's possession to effect a border a search.[395] The traveler then provided this password.[396] In reviewing this aspect of the encounter, the circuit court found no issue with the customs officers' conduct and their actions were reasonable.[397] The decision re-affirms that because border searches are not consensual a lack of cooperation by a traveler should not defeat the endeavor.

Reasonableness in the exercise of electronic border search authority also commands that, absent such extenuating circumstances, as national security concerns, travelers should be aware that their electronic devices are being inspected.[398] Customs officers should make every effort to conduct suspicion-less electronic border searches in the traveler's presence. But it is reasonable for customs officer to make traveler's aware, as was done in *Wanjiku*, of the results of their failure to facilitate such an inspection. Applying and adapting existing statutory authority to allow customs officers to demand that locked devices be unlocked, and to detain, if necessary, locked and encrypted devices, means travelers cannot defeat legitimate government interests in the border domain merely through the use of passwords.

---

[392] 19 U.S.C. § 1462.

[393] *Wanjiku*, 919 F.3d at 477.

[394] *Wanjiku*, at 477.

[395] *Wanjiku*, at 477.

[396] *Wanjiku*, at 477.

[397] *Wanjiku*, at 489.

[398] Customs and Border Protection, *Border Searches of Electronic Devices.*

E. CONCLUSION

Constantly evolving technologies present challenges to maintaining both the effectiveness and reasonableness of government search and seizure authority. Government searches involving such technologies, like modern, mobile electronic devices, have the potential to more greatly intrude on a person's privacy than searches of traditional property. This new type of property, however, has altered and enhanced the ability of individuals to threaten the U.S. and bypass customs laws. The government, within existing authorities, must be allowed to keep pace and even "catch up."[399] Creating special rules for every new technology that is developed is neither possible nor desirable. The result would be uncertainty and problems of logic of the kind pointed out by McAdams in the wake of *Riley*.[400] Any such standard would prove universally unworkable and often be injurious to the public good.[401] Also problematic is ignoring statutory rules and legislative guidance. Important lessons can be learned from Congressional attempts to balance government and personal interests when confronted with evolving technology.[402] Such ignorance leads to rule-making in a vacuum based on narrow perspectives with potentially far-reaching consequences.[403]

A tiered, hybrid-scope-limited electronic border search protocol allows existing rules governing border searches and searches of electronic data to be translated to confront novel issues presented by evolving technology. It fosters perceptions of legitimacy in such searches by recognizing that unlimited access to all electronic data without regard to the rationale underlying the existence of the border search doctrine is untenable. By charting a middle course, the tiered, hybrid-scope-limited approach to electronic border searches respects the intentionally created twin-search paradigm that views a search by a customs officer at the border as substantially different from all others. It, however, does so without needlessly trampling on personal privacy.

---

[399] Clancy, "Fourth Amendment Satisfaction," 44.

[400] McAdams, "*Riley*'s Less Obvious Tradeoff," 128.

[401] See, for example, *Carroll*, 45 S. Ct. 280; *Terry*, 392 U.S. 1; and *Buie*, 494 U.S. 325.

[402] See, generally, Kerr, "The Fourth Amendment and New Technologies."

[403] *Kolsuz*, 890 F.3d at 150–53 (Wilkinson, J., concurring).

With the continuing technological changes of the modern world, electronic border searches are more seminal in their utility in protecting the government's compelling interests than ever before. But a degree of balance must be maintained even when the government's interests hold the trump card. The framework for electronic border searches discussed in this work avoids the crippling pitfall that would be created should the rhetoric of *Riley* be extended to the border search context in the future. The tiered, hybrid-scope-limited framework preserves doctrinal consistency and maintains fidelity to the historic purpose of the border search doctrine. It is also more malleable. This framework is flexible enough to adapt to rapid advancements in technology and property whereby the long-term constitutionality in the application of electronic border search authority can be maintained. A tiered, hybrid-scope-limited construct makes the age-old border search rule, as applied to electronic devices and data, both more reasonable and enduring.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alzahabi, Rasha. "Should You Leave Your Laptop at Home When Traveling Abroad? The Fourth Amendment and Border Searches of Laptop Computers." *Indiana Law Review* 41, no. 1 (2008): 161–86. https://doi.org/10.18060/3928.

Argiriou, Steven L. "Terry Stop Update: The Law, Field Examples and Analysis." Federal Law Enforcement Training Centers. Accessed September 23, 2020. https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/4th-amendment/terrystopupdate.pdf.

Barton, Zach. "What Is a Cloud Application?" *CloudBakers* (blog), April 18, 2018. https://www.cloudbakers.com/blog/what-is-a-cloud-application.

Bates, Philip. "What Is Airplane Mode on IPhone? Everything You Need to Know." MakeUseOf, June 22, 2020. https://www.makeuseof.com/tag/everything-need-know-airplane-mode-iphone-ipad/.

Bector, Sunil. "Your Laptop, Please: The Search and Seizure of Electronic Devices at the United States Border." *Berkeley Technology Law Journal* 24 (2009): 695–718.

Black, Henry C., Joseph R. Nolan, and Jacqueline M. Nolan-Haney. *Black's Law Dictionary: Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern*. 6th ed. St. Paul, MI: West Publishing Group, 1990.

Bohannon, Gina. "Cell Phones and the Border Search Exception: Circuits Split over the Line between Sovereignty and Privacy." *Maryland Law Review* 78, no. 3 (2019): 563–603.

Brady, Maureen E. "The Lost 'Effects' of the Fourth Amendment: Giving Personal Property Due Protection." *Yale Law Journal* 125, no. 4 (2016): 946–1017.

CaseGuard. "Digital Evidence Metadata." Accessed October 5, 2020. https://caseguard.com/evidence-blog/digital-evidence-metadata.

Center for Latin American and Latino Studies. *MS13 in the Americas: How the World's Most Notorious Gang Defies Logic, Resists Destruction*. Washington, DC: American University, 2018. www.https://www.justice.gov/eoir/page/file/1043576/download.

Clancy, Thomas K. *The Fourth Amendment: Its History and Interpretation*. 2nd ed. Durham: Carolina Academic Press, 2014.

———. “Fourth Amendment Satisfaction—The ‘Reasonableness’ of Digital Searches.” *Texas Tech Law Review* 48 (2015): 37–63.

———. “The Framers’ Intent: John Adams, His Era, and the Fourth Amendment.” *Indiana Law Journal* 86 (2011): 979–1617.

Coletta, Christine A. “Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment.” *Boston College Law Review* 48, no. 4 (2007): 971–1007.

Constitution Project. *Suspicionless Border Searches of Electronic Devices under the Border Search Doctrine: Legal and Privacy Concerns with the Department of Homeland Security’s Policy*. Washington, DC: Constitution Project, 2011.

Corbett, Patrick. “The Future of Digital Evidence Searches and Seizures: The Future of the Fourth Amendment in a Digital Evidence Context: Where Would the Supreme Court Draw the Electronic Line at the International Border?” *Mississippi Law Journal* 81 (2012): 1263–1308.

Customs and Border Protection. *Border Searches of Electronic Devices*. Directive No. 3340-049A. Washington, DC: Customs and Border Protection, 2018.

———. “CBP Releases Fiscal Year 2015 Trade and Travel Numbers.” March 4, 2016. https://www.cbp.gov/newsroom/national-media-release/cbp-releases-fiscal-year-2015-trade-and-travel-numbers.

Dam, Kenneth, and Herbert Lin, eds. *Cryptography’s Role in Securing the Information Society*. Washington, DC: National Academies Press, 1996. https://doi.org/10.17226/5131.

Department of Homeland Security. “The Life Saving Missions of ICE.” August 20, 2018. https://www.dhs.gov/news/2018/08/20/life-saving-missions-ice.

Department of Justice. “Electronic Surveillance—Title III Affidavits.” February 19, 2015. https://www.justice.gov/archives/jm/criminal-resource-manual-29-electronic-surveillance-title-iii-affidavits.

Donohue, Laura K. “Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches.” *Yale Law Journal Forum* 128 (2019): 961–1015. https://www.yalelawjournal.org/forum/customs-immigration-and-rights.

Dripps, Donald A. “‘Dearest Property’: Digital Evidence and the History of Private ‘Papers’ as Special Objects of Search and Seizure.” *Journal of Criminal Law and Criminology* 103, no. 1 (2003): 49–110.

———. “The Fourth Amendment and the Fallacy of Composition: Determinacy versus Legitimacy in a Regime of Bright-Line Rules.” *Mississippi Law Journal* 74 (2005 2004): 341–427.

Fayle, Kevin. “Dignity, Privacy and Hard Drives: Laptops and the Border Search Exception to the Fourth Amendment.” *Law-Technology* 41, no. 4 (2008): 1–30.

Flipse, Rachel. “An Unbalanced Standard: Search and Seizure of Electronic Data under the Border Search Doctrine.” *University of Pennsylvania Journal of Constitutional Law* 12, no. 3 (2010): 851–74.

Fontecchio, Ari B. “Suspicionless Laptop Searches under the Border Search Doctrine: The Fourth Amendment Exception That Swallows Your Laptop.” *Cardozo Law Review*, no. 31 (2009): 231–66.

Gilmore, Kelly A. “Preserving the Border Search Doctrine in a Digital World: Reproducing Electronic Evidence at the Border.” *Brooklyn Law Review* 72, no. 2 (2007): 759–97.

Goldschein, Eric. “Following the Cocaine Trail: How the White Powder Gets into American Hands.” Business Insider, December 8, 2011. https://www.businessinsider.com/cocaine-facts-2011-12.

Goodison, Sean E., Robert C. Davis, and Brian A. Jackson. *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/pubs/research_reports/RR890.html.

Harvard Law Review. “The Border Search Muddle.” 132 (2019): 2278–99.

Haselton, Todd. “Many Apps on Your Phone Are Tracking Everywhere You Go—Here’s How to Stop Them.” CNBC, December 12, 2018. https://www.cnbc.com/2018/12/12/how-to-stop-apps-from-tracking-your-location.html.

Immigration and Customs Enforcement. *Border Searches of Electronic Devices*. Directive No. 7-6.1. Washington, DC: Immigration and Customs Enforcement, 2009.

Isaacs, Katelin P. *Retirement Benefits for Federal Law Enforcement Personnel*. CRS Report No. R42631. Washington, DC: Congressional Research Service, 2017. https://fas.org/sgp/crs/misc/R42631.pdf.

Ittig, Judith B. “The Rites of Passage: Border Searches and the Fourth Amendment.” *Tennessee Law Review* 40 (1973): 329–794.

Jarrett, H. Marshall, Michael W. Bailie, Ed Hagen, and Nathan Judish. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Washington, DC: Department of Justice, 2009.

Justice Information Sharing. "Electronic Communications Privacy Act of 1986." Accessed September 18, 2020. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

Kerr, Orin S. "Applying the Fourth Amendment to the Internet: A General Approach." *Stanford Law Review* 62, no. 4 (2010): 1005–49.

———. "An Equilibrium-Adjustment Theory of the Fourth Amendment." *Harvard Law Review* 125, no. 2 (2011): 476–543.

———. "Foreword: Accounting for Technological Change." *Harvard Journal of Law and Public Policy* 36, no. 2 (Spring 2013): 403–8.

———. "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution." *Michigan Law Review* 102, no. 5 (March 2004): 801–88. https://doi.org/10.2307/4141982.

———. "Fourth Amendment Seizures of Computer Data." *Yale Law Journal* 119, no. 4 (2010): 700–24.

———. "Searches and Seizures in a Digital World." *Harvard Law Review* 119, no. 2 (2005): 531–85.

Kerry, Cameron F. "Why Protecting Privacy Is a Losing Game Today—and How to Change the Game." Brookings, July 12, 2018. https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

Kugler, Matthew B. "The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study." *University of Chicago Law Review* 81, no. 3 (2014): 1165–1211.

LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*. Vol. 5. 5th ed. St. Paul, MI: West, 2012.

Lasson, Nelson. *The History and Development of the Fourth Amendment to the United States Constitution*. Baltimore: Johns Hopkins Press, 1937.

Leary, Mary. "The Supreme Digital Divide." *Texas Tech Law Review* 48 (2015): 65–95.

Lee, Cynthia. "Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us about the Fourth Amendment." *Journal of Criminal Law & Criminology* 100, no. 4 (Fall 2010): 1403–94.

Linthicum, David. “The Cloud and the Internet of Things Are Inseparable.” InfoWorld, January 12, 2016. https://www.infoworld.com/article/3021059/cloud-and-internet-of-things-are-inseparable.html.

McAdams, Richard. “*Riley*’s Less Obvious Tradeoff: Forgoing Scope-Limited Searches.” *Texas Tech Law Review* 48 (2015): 97–131.

McLaughlin, Molly. “How Does a Fitbit Work?” Lifewire, February 22, 2020. https://www.lifewire.com/what-is-fitbit-4176010.

Miller, Thomas Mann. “Digital Border Searches after *Riley v. California*.” *Washington Law Review* 90, no. 4 (2015): 1943–96.

Nadkarni, Sid. “‘Let’s Have a Look Shall We?’ A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices.” *UCLA Law Review* 61 (2013): 146–94.

Naked Security. “Border Agents Are Copying Travelers’ Data, Leaving It on USB Drives.” December 13, 2018. https://nakedsecurity.sophos.com/2018/12/13/border-agents-are-copying-travelers-data-leaving-it-on-usb-drives/.

Nowell, Laura. “Privacy at the Border: Applying the Border Search Exception to Digital Searches at the United States Border.” *Federal Communications Law Journal* 71, no. 1 (2019): 85–104.

Office of the Comptroller of the Currency. *Bank Secrecy Act/Anti-Money Laundering: Comptroller’s Handbook*. Washington, DC: Office of the Comptroller of the Currency, 2000.

———. “Bank Secrecy Act (BSA) & Related Regulations.” March 25, 2019. https://www.occ.treas.gov/topics/supervision-and-examination/bsa/bsa-related-regulations/index-bsa-and-related-regulations.html.

———. “Suspicious Activity Reports (SAR).” March 4, 2019. https://www.occ.treas.gov/topics/supervision-and-examination/bank-operations/financial-crime/suspicious-activity-reports/index-suspicious-activity-reports.html.

Ohm, Paul. “The Fourth Amendment in a World without Privacy.” *Mississippi Law Journal* 81, no. 5 (2012): 1309–56.

Park, Eunice. “The Elephant in the Room: What Is a ‘Nonroutine’ Border Search, Anyway? Digital Device Searches Post-*Riley*.” *Hastings Constitutional Law Quarterly* 44 (2017): 277–314.

Peters, Richard, ed. *The Public Statutes at Large of the United States of America, from the Organization of the Government in 1789, to March 3, 1845*. Vol. 1. Boston: Charles C. Little and James Brown, 1845. https://www.loc.gov/law/help/statutes-at-large/1st-congress/c1.pdf.

Pryby, Christopher. "Forensic Border Searches after *Carpenter* Require Probable Cause and a Warrant." *Michigan Law Review* 118, no. 3 (2019): 507–32.

Rana, Nikita, Gunjan Sansanwal, Kiran Khatter, and Sukhdev Singh. "Taxonomy of Digital Forensics: Investigation Tools and Challenges." Cornell University. Accessed November 22, 2020. https://arxiv.org/ftp/arxiv/papers/1709/1709.06529.pdf.

Richman, Sheldon. "TGIF: James Madison: Father of the Implied-Powers Doctrine." Future of Freedom Foundation. Accessed September 5, 2020. https://www.fff.org/explore-freedom/article/tgif-james-madison-father-of-the-implied-powers-doctrine/.

Robles, Alfonso. *Law Course for Customs and Border Protection Officers*. 13th ed. Glynco, GA: Gould Publications, 2004.

Rouse, Margaret. "Cloud Storage." SearchStorage. Accessed September 18, 2020. https://searchstorage.techtarget.com/definition/cloud-storage.

Sales, Nathan A. "Run for the Border: Laptop Searches and the Fourth Amendment." *University of Richmond Law Review* 43 (2009): 1091–1134.

Samuelson, Pamela. "Review: A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy." *California Law Review* 87, no. 3 (1999): 751–78. https://doi.org/10.2307/3481032.

SCOTUS Blog. "*Cotterman v. United States*." Accessed July 9, 2020. https://www.scotusblog.com/case-files/cases/cotterman-v-united-states/.

Sklansky, David Alan. "Too Much Information: How Not to Think About Privacy and the Fourth Amendment." *California Law Review* 102, no. 5 (2014): 1069–1121.

Slobogin, Christopher. "An Original Take on Originalism." *Harvard Law Review* 125 (2011): 14–22.

Smith, Hillel R. *Do Warrantless Searches of Electronic Devices at the Border Violate the Fourth Amendment?* CRS Report No. LSB10387. Washington, DC: Congressional Research Service, 2019. https://crsreports.congress.gov/product/pdf/LSB/LSB10387.

Stengel, Joseph J. "The Background of the Fourth Amendment to the Constitution of the United States." *University of Richmond Law Review* 3, no. 2 (1969): 278–98.

Upright, Scott J. “Suspicionless Border Seizures of Electronic Files: The Overextension of the Border Search Exception to the Fourth Amendment.” *William and Mary Law Review* 51, no. 1 (2009): 291–326.

Wilson, Victoria. “Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States Borders from Bombs, Drugs, and the Pictures from Your Vacation.” *University of Miami Law Review* 65, no. 3 (2011): 999–1025.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California