FLEETING DATA: USING ARTIFICIAL INTELLIGENCE TO MAKE SENSE OF THE BORDER EXCEPTION

BRENDAN SULLIVAN*

* Lieutenant Commander Brendan Sullivan, Judge Advocate, United States Coast Guard. Presently assigned as Deputy Staff Judge Advocate, U.S. Coast Guard Cyber Command, Coast Guard Headquarters, Washington, D.C. The views expressed are those of the author and do not reflect the official policy or position of the U.S. Coast Guard or Department of Homeland Security. Special thanks to Professor David Koplow and Lauren Graham Sullivan for their assistance and insights.

INTRODUCTION

In the information age, smugglers not only conceal tobacco, drugs, or firearms as they cross the border, they carry something more sensational–massive amounts of data that can be transported in small devices. Adversaries want that data to harm U.S. interests with traditional military capability, intelligence, and economic power.[1] Law enforcement stationed at the border is uniquely positioned to protect sensitive information before it absconds to U.S. adversaries who will use it for nefarious purposes. This article proposes developing tools for law enforcement to execute that mission without unreasonably interfering with personal privacy rights.

In 1995, President Clinton took a stand against Iranian President Akbar Hashemi Rafsanjani's attempts to gain nuclear capability by declaring sanctions to rebuff Iran's "unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."[2] Those sanctions were the authoritative underpinning for the 2014 conviction of Ali Saboonchi, who shipped specialized technology to Iran that could be used to develop nuclear weapons.[3] For over a year, federal

1. U.S. adversaries have attempted to build nuclear capabilities by acquiring technology from the U.S., but U.S. adversaries also attempt to undermine U.S. economic strength by stealing U.S. trade secrets. *See* William J. Broad & David E. Sanger, *Relying on Computer, U.S. Seeks to Prove Iran's Nuclear Aims*, N.Y. TIMES, Nov. 13, 2005, at A1; James Risen & Jeff Gerth, *China Stole Nuclear Secrets for Bombs, U.S. Aides Say*, N.Y. TIMES, Mar. 6, 1999, at A1; David E. Sanger & Choe Sang-Hun, *Reckoning with a Nuclear Peril*, N.Y. TIMES, May 7, 2016, at A1; Press Release, Rep. Nadler on Protecting Trade Secrets of American Companies (June 24, 2014), https://nadler.house.gov/news/documentsingle.aspx ?DocumentID=391124 [https://perma.cc/5QK7-LZBV].

2. Exec. Order No. 12957, 60 Fed. Reg. 14615 (Mar. 15, 1995).

3. Government's Response to Defendant's Sentencing Letters at 11, United States v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014) (No. PWG-13-0100), 2015 WL 471760, at *10–11 (Jan. 27, 2015). In 2016, Saboonchi was released along with an Iranian national convicted of providing information to Iran that helped it launch its first satellite. Their release was pursuant to an exchange that occurred once Iran met its initial obligations under a negotiated arrangement that would seek to end sanctions in exchange for Iran seizing its nuclear enrichment activities. *See* Ian Duncan, Ramin Mostaghim, Tracy Wilkinson & Patrick J. McDonnell, *Parkville Man Released from U.S. Prison in Deal to Free Americans Held in Iran*

investigators tracked Saboonchi but were unable to collect enough evidence to prosecute him until he made a one-day trip across the Canadian border with his wife.[4] Upon his return to the United States, Customs officials seized Saboonchi's personal electronic devices and conducted a forensic search, which revealed evidence that he conspired with businessmen in Iran to transport filters, valves, thermocouples, and other goods that could be used to develop nuclear technology.[5] The government's case against Saboonchi relied on evidence obtained without probable cause or a warrant to search his personal electronic devices. The government's authority to search Saboonchi's devices stemmed from the border exception to the warrant requirement.[6]

As the information age progresses and personal electronic devices hold increasing amounts of data, courts and Congress are weighing in on how the border exception should be applied in the digital context. On one hand, there is empathy for the notion that phones and other devices serve as our most intimate confidants and, therefore, should not be open to searches at the border without some level of suspicion that the device contains illicit material. On the other hand, there is justifiable rationale that personal privacy interests in data maintained on our devices must give way to some consideration for national security concerns.

It is time for Congress to establish the framework and the scope of authorized electronic border searches at the border. Congressional intervention is necessary because the federal judiciary is divided on how law enforcement should treat devices like Saboonchi's. Meanwhile, the threat presented by these devices is increasingly concerning.

The federal judiciary's position on the level of privacy warranted for electronic data at the border is spread across a confusing patchwork of ambiguity. The following discussion advocates that Congress should act to set a singular, enduring standard for electronic data searches at the border so that courts, law enforcement, and the public know what travelers should expect when they enter or leave the United States. This article provides context for understanding the legal basis for warrantless searches at the border. It then uses this context to propose legislation that can leverage developing technology to search devices at the border while limiting the extent to which personal data is exposed to law enforcement bias. In many ways, electronic device searches conducted at the border present the perfect opportunity to secure national interests while limiting personal bias that

---

with Another to Reportedly Follow, BALTIMORE SUN (Jan. 17, 2016, 9:47 AM), https://www.baltimoresun.com/business/bs-md-iran-prisoners-20160116-story.html [https://perma.cc/44D9-AKH6].

4. United States v. Saboonchi, 990 F. Supp. 2d 536, 539, 542–44 (D. Md. 2014).

5. *Id.* at 540, 542; Superseding Indictment at 3–9, United States v. Ali Saboonchi, 990 F. Supp. 2d 536, 540 (D. Md. 2014) (No. PWG-13-0100).

6. *Saboonchi*, 990 F. Supp. 2d at 540, 554.

may be consciously or unconsciously applied to officer discretion. By coupling forensic technology with artificial intelligence software, potential threats can be identified with image identifiers and key search terms, phrases, and images. The amount of data crossing the border and the diverse populations that data belongs to offer an opportunity to study the analytical process for surveying information for threats while limiting the concerning biases that might influence the decision to collect and retain that data.

Section I of this paper looks at the development of the border exception and considers its application in an increasingly digital world. As technology evolves, so has its use by state adversaries and illicit networks attempting to conceal information and communications. Accordingly, law enforcement tactics to access this information must also evolve. When law enforcement tactics infringe on perceived privacy interests, courts try to balance those interests against the government's interest in preserving national security. Ultimately, Congress is better positioned than the courts to identify reasonable solutions. Congress has a unique perspective on the public's interest in personal information on their electronic devices and it also has distinct authority over national security matters. Its perspective and its authority should be leveraged to find solutions that can identify criminal, economic, and military threats crossing the border.

Section II explores circumstances where a border search requires law enforcement to have suspicion of illegal activity and addresses whether those circumstances are analogous to an electronic device search. When facts and circumstances surrounding a traveler's movement across the United States border call for law enforcement actions that demand suspicion of illicit activity, the Supreme Court labels the search as "non-routine."[7] The origins of the Court's distinction between routine and non-routine searches at the border is founded in the principle that a traveler should not be subject to undue delay at the border.[8] The border exception was designed to efficiently survey items crossing the border before they can cause harm to the populace. Technology can reduce delay by rapidly identifying personal property that merits closer examination. Moreover, forensic searches identifying concerning information can be vetted for bias to ensure that law enforcement's basis for suspecting evidence of illegal activity is based upon appropriate factors.

Section III reviews proposed solutions to the problem of protecting privacy interests and national security interests at the border. While some view the border exception as a limited authority that only applies to

7. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985) (holding that customs officials must reasonably suspect illegal activity to detain a traveler for a search and inspection that is not routine).

8. *Id.*

physical contraband crossing an international boundary,[9] others view the border as a threshold of sovereignty and a final opportunity to thoroughly vet travelers for national security threats.[10] Technology will not provide a resolution to this divide, but it can provide a mechanism for definitively distinguishing between contraband and other evidence that some argue is not "tethered" to the border exception.[11]

Since at least 2009, Congress recognized the tension between privacy interests and national security interests in digital data at the border.[12] While some congressional proposals attempting to address the problem advanced sound suggestions, they are missing details that will reconcile the tension between privacy and national security interests. Each proposal presented thus far has advocated to restrict law enforcement and add reporting responsibilities, rather than equip border enforcement with tools to identify national security threats in a manner that respects individual rights. Legislation that encourages federal agencies to use technology will do more to protect the border while simultaneously protecting those rights.

Section IV advocates for legislation to address divided views on digital device searches at the border. The proposal outlined in this section will consider personal privacy interests in data crossing the border, while providing a mechanism for law enforcement to identify national security threats. The proposed legislation uses artificial intelligence to ferret out data that presents the greatest concern for U.S. security. Some experts criticize artificial intelligence and advanced programing methods as being biased, but such criticism is largely supported by concerns with systems that do not review and continually test data.[13] Given the number of people and devices crossing the border on a daily basis, the border is a perfect platform for artificial intelligence. By continually testing, administering, and reporting on artificial intelligence aided searches at the border, agencies can study and minimize bias, thus protecting privacy interests and defending against

---

9. Brief of Constitutional Accountability Center as Amicus Curiae in Support of Plaintiffs, Alasaad v. Nielsen, 419 F. Supp. 3d 142 (D. Mass. 2019) (No. 17-cv-11730-DJC).

10. *See generally* United States v. Kolsuz, 890 F.3d 133, 143 (4th Cir. 2018) (arguing that a device search at the border leading to evidence of illegal firearms exports "goes to the heart" of the Fourth Amendment exception to the warrant requirement at the border).

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

12. *See*, *e.g.*, Border Security Search Accountability Act of 2009, H.R. 1726, 111th Cong. (2009); Securing our Borders and our Data Act of 2009, H.R. 239, 111th Cong. (2009).

13. Artificial intelligence creates a continuum that "as a function of how much privacy you want and how much data you have" can improve the level of accurate restrictions on privacy exponentially with more data. *The Cyberlaw Podcast: Ethical Algorithms with Michael Kearns and Aaron Roth*, STEPTOE & JOHNSON LLP (Dec. 5, 2019) (downloaded using iTunes).

discriminatory application of the warrant exception. If successful, programing practices developed at the border could be used for broader law enforcement initiatives.

I. THE PURPOSE OF THE BORDER EXCEPTION IN A DIGITAL WORLD

Technology has exposed disparate beliefs on why the border exception exists. Digital privacy adds a new dimension to border search authority, but "[i]t's the border, not the technology that 'matters.'"[14] In one of the first cases to address law enforcement's authority to search cross-border information, the Supreme Court held that "compulsory discovery . . . compelling the production of . . . private books and papers, to convict [the defendant] of a crime, or to forfeit his property is contrary to the principles of a free government."[15] Subsequent courts, however, find paramount interest in combatting crime, advancing the position that "the legitimate interest of society in enforcement of its laws . . ." protects personal liberties.[16]

Like most legal issues, the question of where the law is going depends, in part, on where it has been. The debate over electronic data searches at the border starts with what is in agreement–the text of the Fourth Amendment. That Constitutional provision ensures:

> [t]he 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.[17]

What is reasonable in the search and seizure context depends upon the circumstances as well as consideration of "whether the search was justified at its inception and whether, as conducted, it was reasonably related in scope and circumstances that justified the interference in the first place."[18]

The Supreme Court gives individualized treatment to the Fourth Amendment's Reasonableness Clause and Warrant Clause.[19] The

14. United States v. Cotterman, 709 F.3d 952, 976 (9th Cir. 2013) (Callahan, J., dissenting) citing majority at 965.

15. Boyd v. United States, 116 U.S. 616, 631–32 (1886).

16. *The Life and Times of* Boyd v. United State*s (1886-1976)*, 76 MICH. L. REV. 184, 212 (1977) (citing Couch v. United States, 409 U.S. 322, 336 (1973)).

17. U.S. CONST. amend. IV. *See also* Riley v. California, 134 S. Ct. 2473, 2482 (2014) (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness'").

18. New Jersey v. T.L.O., 469 U.S. 325, 326 (1985).

19. *See* Terry v. Ohio, 392 U.S. 1, 20 (1968).

Reasonableness Clause, conferring the right to be secure against unreasonable searches, demands probable cause for issuance of a warrant.[20] The Reasonableness Clause and the Warrant Clause converge in circumstances where a warrant, issued by a detached neutral magistrate, is required to determine if a search is reasonable.[21] However, there is an important distinction between the two clauses, especially in the context of an extraterritorial search where a warrant is not required.[22] Even where the warrant requirement does not apply, the government is not relieved of its burden to conduct searches under reasonable terms.[23]

Not all searches demand a warrant. Some warrantless searches, like a Terry Stop, require law enforcement to identify suspicion of illegal activity.[24] Other warrantless searches, like sobriety checkpoint stops, can be conducted without identifying any suspicion of illegal activity.[25] Searches at the border generally fall into the latter category because they are "reasonable simply by virtue of the fact that they occur at the border."[26] They are given special treatment in this regard because border searches recognize the "right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country."[27] The Supreme Court endorses this broad law enforcement authority at the international boundary with Canada and Mexico, but it also applies at airports, seaports, or other areas that may constitute a functional equivalent of the border.[28] In effect, the border exception may apply thousands of miles from an international boundary.

Proponents of a warrant requirement for all digital devices at the border argue that law enforcement's employment of the exception should be limited to interdicting physical contraband, not digital information.[29] This proposition erodes the principles the Fourth Amendment was built

---

20. *Id.*

21. *Id.* at 20–21.

22. *See generally*, United States v. Verdugo-Urquidez, 494 U.S. 259 (1990) (holding that Fourth Amendment protections do not apply to foreign citizens in a foreign state).

23. *Id.* at 278 (Kennedy concurring).

24. *Terry*, 392 U.S. at 30–32 (holding that law enforcement may temporarily seize an individual without a warrant when there is reasonable suspicion of criminal activity).

25. *See*, *e.g.*, Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (holding sobriety check points constitutional); New Jersey v. T.L.O., 469 U.S. 325, 326 (1985) (holding that school administrators may conduct suspicionless searches of a student's bag).

26. United States v. Ramsey, 431 U.S. 606, 616 (1977).

27. *Id.* at 620.

28. Almeida-Sanchez v. United States, 413 U.S. 266, 268, 272 (1973).

29. Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant-Appellant and Reversal at 33, United States v. Williams, No. 16-cr-249-WJM, 2017 WL 11491959 (D. Col. Sept. 25, 2017) (No. 16-cr-249-WJM).

upon by treating evolving technological data as distinct from other forms of contraband and evidence scrutinized at the United State's sovereign border. Child sexual abuse material is frequently cited as an example of contraband being concealed in a digital format,[30] but trade secrets and sensitive national security information can easily be concealed in digital format as well.[31] There are so few circumstances where contraband would present in non-digital format that digital searches of some form must be part of the modern understanding of the border exception. It makes little sense that a traveler could be searched without suspicion of engaging in illegal activity and arrested for carrying illegal documents, but if the traveler takes a photo of those documents, they are suddenly subject to different Fourth Amendment protections. The United States retains a sovereign interest in preventing those problems from evading border authorities regardless of the format used to transport them.

The previously mentioned example of an individual taking a photo to hide otherwise discoverable information highlights how technology not only expands access to information, it creates a new dimension that is hard to analogize to historical Fourth Amendment concepts. The high volumes of information accessible on a device reveals our movements, our friendships, and our secrets. It is highly unlikely the Fourth Amendment drafters could have foreseen today's circumstances, where travelers carry nearly every personal detail of their life with them in a device the size of a pack of cigarettes. The most logical way of addressing the capability to conceal and transport vast amounts of information with technology is ensuring that law enforcement is equally capable of vetting devices at the border without intruding on personal privacies. This proposed adaptation should take into consideration the reason why the law created an exception to the Fourth Amendment.

A. How Have Fourth Amendment Rights at the Border Developed?

In 1790, the United States was eager to work its way out of Revolutionary War debt and build itself into a global economic

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

31. In 2019, a criminal complaint was issued against a U.S. citizen alleging that over the course of several years he was attempting to pass national security information to the Chinese government using a Secure Digital (SD) card. Even though the perpetrator was interdicted before information was passed to the Chinese government, the SD card he used would have been smuggled across the U.S. border at some point. *See* Jacob Schulz, *DOJ Charges American Citizen with Acting as an Illegal Agent of China*, LAWFARE BLOG (Tuesday, Oct. 1, 2019, 3:19 PM), https://www.lawfareblog.com/doj-charges-american-citizen-acting-illegal-agent-china [https://perma.cc/4MEE-63XB].

competitor.[32] Despite the country's best efforts to overcome flaws in colonial taxation, the Founding Fathers soon realized how quickly debt accrues. As a result, they sought to combat against the primary national security concern at the time–smuggling.[33]

To build the nation's economy, the first Congress set out to impose tariffs on imports, but there was no mechanism in place to enforce those tariffs.[34] Recognizing that there were fleeting opportunities to capture evidence of goods smuggled across the border, Congress authorized searches and seizures of "any ship or vessel, goods, wares or merchandise."[35] Because this authority was enacted within two years of the Constitution being ratified, scholars argue that the Framers expected there would be circumstances calling for warrantless searches.[36]

Merchandise carried in the holds of ships that can easily escape the jurisdiction of border enforcement offers a baseline example of reasonable suspicionless searches. Expanding on this principle, the Supreme Court in *Carroll v. United States* recognized that the "Fourth Amendment does not denounce all searches or seizures, but only such as are unreasonable."[37] To determine the scope of a reasonable search, the Court looks to the justifiable conduct of law enforcement officers under the circumstances at hand rather than whether it was reasonable to obtain a warrant under those circumstances.[38]

Like goods on a ship, electronic data carried across sovereign borders also has fleeting characteristics. Electronic data is easily erased, transferred, and concealed for nefarious purposes.[39] From a forensics standpoint, identifying criminals who use technology for nefarious means is so challenging that most information technology experts advocate for

---

32. THOMAS K. MCCRAW, THE FOUNDERS AND FINANCE: HOW HAMILTON, GALLATIN, AND OTHER IMMIGRANTS FORGED A NEW ECONOMY 47–48 (2012). *See also* Alanna Ritchie, *Timeline of U.S. Federal Debt Since Independence Day 1776*, DEBT.ORG (July 4, 2013), https://www.debt.org/blog/united-states-federal-debt-timeline/ [https://perma.cc/4GUL-KZRD] (remarking on the increase of national debt from over $2 million during the Revolutionary War and increasing to $43 million two years later, and then, rising to $119.2 million by 1815).

33. MCCRAW, *supra* note 32, at 91.

34. *See* Greg Shelton, *The United States Coast Guard's Law Enforcement Authority Under 14 U.S.C. § 89: Smugglers' Blues or Boaters' Nightmare?*, 34 WM. & MARY L. REV., 933, 938–39 (1993).

35. United States v. Ramsey, 431 U.S. 606, 616 (1977) (quoting the Act of July 31, 1789, c. 5, 1 Stat. 29 § 24).

36. Akhil Reed Amar, *Terry and Fourth Amendment First Principles*, 72 ST. JOHN'S L. REV. 1097, 1104–05 (1998).

37. Carroll v. United States, 267 U.S. 132, 147 (1925).

38. United States v. Rabinowitz, 339 U.S. 56, 66 (1950).

39. *See* Marcell Gogan, *The 8 Most Disturbing Data Breaches of 2018*, IOT FOR ALL (Mar. 6, 2019), https://www.iotforall.com/top-8-most-disturbing-data-breaches-of-2018/ [https://perma.cc/26BT-TGDE].

defensive measures rather than criminal enforcement in order to prevent information loss.[40] Border searches present a unique opportunity to confront travelers that are in possession of illegal content and find information like the type Ali Saboonchi carried. Digital data transported by travelers may not be contraband of the type crossing the border in 1790, but it is information that the United States wants to protect as it faces one of the primary national security threats of today–nuclear proliferation.[41]

B. Border Policy

In an effort to siphon out threats to national security, border authorities try to maintain pace with evolving technologies, but the process of extracting and investigating electronic data can be complicated and time consuming.[42] Improved encryption techniques make it more difficult for law enforcement to bypass security on phones and portable devices. In some cases, it might not be possible to extract data from sophisticated devices and, even when it is possible, extraction takes time and resources.[43]

In 2009, Customs and Border Protection (CBP) recognized that accessing data on portable devices is increasingly complex and, as a consequence, announced a controversial policy that permitted border officials to hold digital media devices for the period of time necessary to conduct a forensic search through electronic data.[44] CBP's policy

---

40. Nickson Menza Karie & Simon Mania Karume, *Digital Forensic Readiness in Organizations: Issues and Challenges*, 12 J. DIGITAL FORENSICS SEC. & L. 43, 43–51 (2017).

41. The National Counterintelligence and Security Center ranks nuclear technology as a high priority target of foreign intelligence collectors. NAT'L COUNTERINTELLIGENCE AND SEC. CTR., FOREIGN ECONOMIC ESPIONAGE IN CYBERSPACE 11 (2018), https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf [https://perma.cc/ZC7G-5WF7].

42. *See* United States v. Cano, 934 F.3d 1002, 1020 (2019) (citing United States v. Wanjiku, 919 F.3d 472, 477 (7th Cir. 2019) (distinguishing between a preview, which may take one to three hours, versus a full examination, which may require months)).

43. *See, e.g.*, Nicole Perlroth, *What is End-to-End Encryption? Another Bull's-Eye on Big Tech*, N.Y. TIMES (Nov. 19, 2019), https://www.nytimes.com/2019/11/19/technology/end-toend-encryption.html [https://perma.cc/JNN8-H2AV]. In 2016, the Manhattan District Attorney reported that the city's cyberlab was unable to unlock 175 phones in its possession with potential evidence in them that could be used to prosecute crimes. *It's Not Just the iPhone Law Enforcement Wants to Unlock*, NASHVILLE PUB. RADIO (Feb. 21, 2016, 7:57 AM ET), https://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock [https://perma.cc/YZC2-UBUR].

44. *See generally* Victoria Wilson, Note, *Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States Borders from*

implemented internal rules as a check on law enforcement's basis for holding the device, but there were no set retention timelines.[45] That same year, the House of Representatives was unsuccessful in passing legislation that would require rulemaking to define the number of days border authorities could hold a device without probable cause.[46]

People cannot be detained at the border for prolonged periods of time without suspicion of illegal activity, but there is no constitutional or legislative restriction on the amount of time a traveler's device can be retained.[47] Ali Saboonchi, who crossed the Canadian border in 2012, had his phone held for a period of nine days.[48] In some cases, electronic devices have been retained for fifty-six days.[49] While the law does not dictate the time or manner for law enforcement authorities holding electronic devices at the border, authorities impose internal policy through amended rules which provide that searches should be completed within thirty days and approved by a supervisor every fifteen days after.[50]

In addition to self-imposed restrictions on the length of time a device will be held, border policy also sets controls on the scope of a device search. In 2017, the Acting Secretary of Homeland Security announced that authority to search digital devices at the border is limited to the data that is physically present at the border.[51] It, therefore, does not include information that might be stored on a cloud or in a server located in some place that is presumably miles away from the border.[52] While the policy avoids broad access to information not being physically transported across the border at the time of the search, distance from the border does not always define authority to conduct a border search. As some courts have held, warrantless searches may be reasonable even when contraband is seized far from the

---

Bombs, Drugs, and the Pictures from Your Vacation, 65 U. MIAMI L. REV. 999 (2011).

45. *See* U.S. CUSTOMS & BORDER PROTECTION, CBP DIRECTIVE NO. 3340-049, BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION (2009).

46. H.R. 1726, 111th Cong. (2009).

47. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 541, 534–44 (1985).

48. United States v. Saboonchi, 990 F. Supp. 2d, 536, 540 (D. Md. 2014).

49. Alasaad v. Nielsen, 419 F. Supp. 3d 142, 150 (D. Mass. 2019).

50. U.S. IMMIGR. & CUSTOMS ENFORCEMENT, DIRECTIVE 7-6.1, BORDER SEARCHES OF ELECTRONIC DEVICES para. 8.3 (2009).

51. *Q&As Attributed to Kevin McAleenan on CBP Border Searches of Personal Electronic Devices*, AM. IMMIGR. LAW. ASS'N (June 20, 2017), https://www.aila.org/infonet/cbp-border-searches-of-personal-electronic-devices [https://perma.cc/YXW9-AYBF].

52. In 2018, CBP amended its policy to align with the Acting Secretary's position, requiring that "officers may not intentionally use the device to access information that is solely stored remotely." U.S. CUSTOMS & BORDER PROTECTION, CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES, § 5.1.2. (2018).

border, so long as there is reason to believe that it was transported across the border in virtually the same condition as it is at the time of the search.[53] Authority to conduct a search without a warrant is justified by the fact that there are fleeting opportunities to identify data before it does harm.[54] Based on these same principles, a warrantless search may be reasonable in circumstances where digital data on a server may have crossed the border.[55]

C. Balancing Governmental Interests

Determining when a warrantless search is justified requires a balancing test that weighs governmental interest in the intrusion against individual privacy interests.[56] As criminal endeavors evolve, courts undertake this balancing, recognizing that there are circumstances where the government's prosecutorial interest is increased.[57] At the border, the "interest in preventing entry of unwanted persons and effects is at its zenith . . . ."[58] Border search authority is, therefore, unique among Fourth Amendment exceptions because it addresses the broader concerns of sovereign security, rather than imminent threats in isolated circumstances.[59] Personal interests are also diminished at the border because travelers have an expectation that their belongings will be subject to search by law enforcement.[60] As a consequence, governmental concerns are "struck much more favorably . . . at the border" because sovereign interests are at stake, and personal privacy interests are less than they may be elsewhere.[61] The balancing test starts with extra weight afforded to the government when balanced against the personal privacy interests of a traveler entering or departing the country.

Though there is precedent to support the notion that law enforcement at the border are afforded special dispensation, some have

---

53. *See, e.g.*, United States v. Bilir, 592 F.2d 735, 739–41 (4th Cir. 1979) (applying the extended border doctrine to a warrantless search miles from a port of entry). Notably, the Ninth Circuit and the D.C. District Court distinguished the extended border doctrine from searches of electronic devices at the border. United States v. Jae Shik Kim, 103 F. Supp. 3d 32, 58 (D.C. Cir. 2015); United States v. Cotterman, 709 F.3d 952, 961–62 (9th Cir. 2013).

54. *Cotterman*, 709 F.3d at 960 (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977)).

55. *See*, *e.g.*, United States v. Delgado, 810 F.2d 480, 484 (5th Cir. 1987) (holding that a warrantless search is valid where there is "reasonable certainty" that contraband in a vehicle crossed the border and that conditions did not change since the time the vehicle crossed the border).

56. Terry v. Ohio, 392 U.S. 1, 20–22 (1968).

57. *See generally id.*

58. United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

59. *See* United States v. Ramsey, 431 U.S. 606, 620–22 (1977).

60. United States v. Montoya de Hernandez, 473 U.S. 531, 539–40 (1985).

61. *Id.*

noted that when it comes to determining government's interest in phones and other personal devices, "Supreme Court precedent affords more Fourth Amendment protection to digital information than many other kinds of property."[62] This assertion is based on two recent cases involving information on cell phones, both ruling in favor of privacy rights over law enforcement interests. In one case, the Court rejected law enforcement authority to track cell phone locations without a warrant.[63] The other case resulted in the Court denying law enforcement the authority to search a cell phone incident to arrest.[64] Notably, neither of these cases implicated border search authority. Therefore, the weight of their relevance in this context is uncertain.

Previous attempts to balance interests have resulted in uneven outcomes. While Ali Saboonchi's case resulted in a conviction, other cases, including one revealing Iran sanction violations through forensic device extraction at the border, resulted in evidence being suppressed because law enforcement lacked reasonable suspicion.[65] Conversely, some courts have held that suspicion of illicit activity is not required to search a device with forensic tools at the border.[66] To avoid parsing standards at the border, law enforcement and the public would be better served if Congress enacted legislation to identify a method for securing the country from threats while protecting important Fourth Amendment doctrine that establishes well-reasoned exceptions to the warrant requirement. One way of preserving exceptions to the warrant requirement while also preserving Fourth Amendment rights is to authorize suspicionless electronic device searches at the border, provided the searches are conducted with technology that scans devices for threats while preserving privacy interests. Conducting searches with technology under specified parameters would avoid significant impacts on constitutional precedent, while shielding personal information from a border officer's scrutiny.

D. What's Reasonable When it Comes to Technology These Days?

"[B]ecause the ultimate touchstone of the Fourth Amendment is 'reasonableness,' the warrant requirement is subject to certain exceptions."[67] Reasonable interests in privacy can have different contexts in

---

62. *Criminal Procedure – Forensic Searches of Digital Information at the Border – Eleventh Circuit Holds That Border Searches of Property Require No Suspicion.* – United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018)*, 132 HARV. L. REV. 1112, 1112 (2019).

63. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

64. Riley v. California, 573 U.S. 373, 401 (2014).

65. *See* United States v. Jae Shik Kim, 103 F. Supp. 3d 32, 59 (D.C. Cir. 2015).

66. United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018).

67. Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

the commercial market than in criminal law; however, the amount of information available to commercial interests is an informative factor that courts should consider. The commercial market has a firm grip on almost all the information used on our phones and portable devices.[68] Recent data shows that only nine percent of Americans feel they have "a lot" of control over their personal data collection and its use.[69] Yet, a very small number of Americans change their behavior to avoid being tracked.[70] These expectations are important for courts and legislatures to keep in mind when balancing national security and personal privacy interests. There is no reason to believe that law enforcement standards will mirror the low expectations of data privacy in commercial markets.[71] However, where there is an expectation that information maintained on a phone or personal device will be disseminated through commercial markets, the line between personally held information and information available to the public becomes thinner.

II. IS A DEVICE SEARCH AS INTRUSIVE AS A STRIP SEARCH?

Electronic device searches at the border are generally labeled by courts in one of two categories: routine searches or non-routine searches.[72] Routine border searches may be executed without suspicion of illicit activity.[73] They are reasonable because they are conducted at the border, and courts understand that personal privacy interests must give way to a limited search and inspection when a traveler enters the country.[74] Case law established a second category of cases referred to as "non-routine" which include instances where a traveler is detained at the border for a prolonged

---

68. *See* Kristina Libby, *The Data Decade: How We Were Bought and Stolen in the 2010s*, POPULAR MECHANICS (Dec. 10, 2019), https://www.popularmechanics.com/technology/security/a30173991/2010s-data-cybersecurity-decade-review/ [https://perma.cc/MA7Q-WMW8].

69. MARY MADDEN & LEE RAINIE, AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY AND SURVEILLANCE, PEW RESEARCH CENTER (2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [https://perma.cc/CUW7-C4SC].

70. *Id.*

71. COMMITTEE ON PRIVACY IN THE INFO. AGE, NAT'L RES. COUNCIL, ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE 253–54 (James Waldo et al. eds., 2007).

72. In *Bryan v. United States*, Judge Roth explained that "[i]n view of the government's interests, [courts] 'have long held that routine searches at our nation's borders are presumed to be reasonable under the Fourth Amendment.' . . . In contrast, 'nonroutine searches . . . require reasonable suspicion.'" 913 F.3d 356, 361 (3d Cir. 2019) (footnotes omitted) (quoting Bradley v. United States, 299 F.3d 197, 201 (3d Cir. 2002)).

73. United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

74. United States v. Ramsey, 431 U.S. 606, 616 (1977).

period of time or is subject to personally invasive searches.[75] Those searches must be justified by reasonable suspicion.[76]

Currently, there is a circuit split on whether forensic searches of electronic media at the border are routine searches.[77] In some jurisdictions, electronic data has been determined to be so personal that courts have found searching portable devices with forensic tools constitutes a non-routine search, requiring the same level of suspicion needed to conduct a strip search, body cavity search, or an x-ray search at the border.[78] In contrast, in upholding Karl Touset's conviction for purchasing large amounts of child pornography, the Eleventh Circuit held that even though reasonable suspicion existed to search his device, border enforcement authorities were not required to articulate any suspicion of illicit activity before searching an electronic device at the border.[79] The court reasoned that the constitutional exception to the warrant requirement at the border is well-established and silent on the subject of searching electronic devices. [80] Therefore, if the legislature deems it appropriate to afford citizens greater protections by restricting warrantless searches of electronic devices at the border, Congress, rather than the courts, should be tasked with recognizing those protections.[81]

Legislation presents an opportunity to settle the law with mechanisms that protect national security interests and privacy interests simultaneously. Instead of limiting access to forensic technology, the law can leverage technology while encouraging innovative ways of searching electronic devices with limited bias and personal scrutiny. By enacting

---

75. *Was Border Search Routine, Non-Routine, or Did it Even Matter?*, QUINLAN SEARCH AND SEIZURE BULL., (Thomson Reuters, St. Paul, Minn.) Sept. 2002, at 1.

76. *Id.*

77. Gina R. Bohannon, Note, *Cell Phones and the Border Search Exception: Circuits Split over the Line between Sovereignty and Privacy*, 78 MD. L. REV. 563, 578–85 (2019).

78. As will be discussed below, in *Montoya de Hernandez*, the Supreme Court held that detaining a traveler at the border beyond a routine customs search and inspection requires reasonable suspicion of illicit activity. 473 U.S. 531, 541 (1985). In so holding, the Court focused on the length of the traveler's detention, rather than the fact that Customs officials conducted a strip search, body cavity search, and an x-ray search. *Id.* at fn. 4, 542–43. Nonetheless, courts frequently focus on the personal invasiveness of the traveler's search in that case, rather than the amount of time she was detained. *See*, *e.g.*, United States v. Cano, 934 F.3d 1002, 1012, 1015 (9th Cir. 2019); United States v. Braks, 842 F.2d 509, 512–15 (1st Cir. 1988) (relying on *Montoya* to establish a six-factor test to analyze the level of intrusiveness existing when a Customs official requests a passenger to lift up her skirt revealing packages of heroin concealed in a girdle).

79. United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018).

80. *Id.* at 1236–37.

81. *Id.*

legislation that uses forensic technology to search for threatening data on personal devices, the law can avoid creative legal solutions that parse out well-grounded Constitutional principles.

A. Routine and Non-Routine Border Searches

The concept of a non-routine search originated over thirty years ago when law enforcement responded to the "War on Drugs" by increasing its scrutiny of travelers crossing the United States border.[82] In 1983, Rosa Elvira Montoya de Hernandez flew from Colombia to Los Angeles with eighty-eight cocaine filled balloons concealed in her alimentary canal.[83] After a ten-hour flight, she was detained for an additional sixteen hours before customs officials sought a court order to conduct a pregnancy test, an x-ray, and a rectal examination.[84] Based on these facts, the Supreme Court held that customs authorities had engaged in a non-routine border search and, as a result, they needed to show reasonable suspicion that the traveler was violating a law as she crossed the border.[85]

Almost twenty years later, the Court held that customs officials engage in a routine border search when they remove a vehicle's fuel tank and inspect it for contraband, and therefore, a showing of reasonable suspicion is not required to dismantle a traveler's car.[86] In that case, a Ford Taurus station wagon crossing the U.S.-Mexico border at the Otay Mesa Port of Entry was diverted to secondary screening where customs officials unbolted the fuel tank, removed the fuel hoses, hammered off a patch, and discovered over eighty-one pounds of drugs.[87] Comparing the government's interest in excluding unwanted persons and effects at the border against the minimal privacy interest in the contents of a fuel tank, the Court held that customs officials did not need to suspect the vehicle operator of illicit activity before taking the car's fuel tank apart.[88] This routine border search of a vehicle's fuel tank, contrasted against the detention and physical examination of a traveler flying into the United States, set the precedential boundary for distinguishing between routine searches and non-routine searches.

---

82. LEIF RODERICK ROSENBERGER, AMERICA'S DRUG WAR DEBACLE 22, 31 (1996).

83. United States v. Montoya de Hernandez, 473 U.S. 531, 532–33 (1985).

84. *Id.* at 533, 535.

85. *Id.* at 538, 541. Even though the holding in *United States v. Montoya de Hernandez* had more to do with the amount of time the traveler was detained, courts of appeal have interpreted the routine verses non-routine distinction established in that case by considering the level of personal intrusiveness imposed. *See*, *e.g.*, United States v. Brak, 842 F.2d 509, 512–14 (1st Cir. 1988).

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

87. *Id.* at 150–51.

88. *Id.* at 153–55.

B. Does Technology Make the Search More Intrusive or Less Intrusive?

To date, no court has entirely denied border officials the ability to review the contents of a phone or other electronic device pursuant to the border exception. Therefore, there remains an open question on how detailed law enforcement's search can be. As mentioned, some devices have been seized at the border and held for as long as fifty-six days.[89] Barring reasonable suspicion of a crime, some courts only authorize border authorities to take a "quick look" at electronic devices.[90]

Apart from temporal distinctions, some courts distinguish between manual searches and forensic searches.[91] For those courts, connecting a traveler's electronic device (or parts of it) to equipment to extract information or data constitutes a forensic search.[92] A manual search may be conducted without suspicion, allowing border officials to look through the device without the aid of forensic software, however law enforcement is prohibited from connecting the device to equipment without reasonable suspicion that illegal activity is afoot.[93] Presumably, these courts limit law enforcement's access to data obtained using forensic technology because it potentially exposes personal information that may not otherwise be accessible with a "quick look."[94]

This distinction is reflected in CBP's current policy of dividing authorized searches into "Basic Searches" and "Advanced Searches."[95] Basic Searches are made without connecting the device to equipment whereas Advanced Searches require the analyzer to connect the device to "external equipment, through a wired or wireless connection, . . . not merely to gain access to the device, but to review, copy, and or analyze its contents."[96] Basic searches may be conducted without suspicion, but the policy requires reasonable suspicion of an illegal activity before officers conduct an Advanced Search.[97]

Technology can be used to enhance a broad spectrum of capabilities that are not well reflected in current jurisprudence, especially when distinguishing between forensic and non-forensic searches. At a

---

89. United States v. Sabanoochi, 990 F. Supp. 2d 536, 559, 569 (D. Md. 2014).

90. *See*, *e.g.*, United States v. Cotterman, 709 F.3d 952, 960–61 (9th Cir. 2013).

91. United States v. Cano, 934 F.3d 1002, 1016 (9th Cir. 2019).

92. Wayne Jansen & Rick Ayers, *Forensic Software Tools for Cell Phone Subscriber Identity Modules*, CONF. ON DIGITAL FORENSICS, SEC. & L. 99 (2006).

93. *Cano*, 934 F.3d at 1016 (citing *Cotterman*, 709 F.3d at 968).

94. *See*, *e.g.*, *Cotterman*, 709 F.3d at 960–61.

95. *See* CBP DIRECTIVE NO: 3340-049A, *supra* note 52, at §§ 5.1.3–5.1.4.

96. *Id.*

97. *Id.*

minimum, a "forensic extraction" can be broken down into five levels.[98] Some extraction methods simplify access to basic information such as text messages, pictures, and call logs, while others enable forensic examiners to bypass password requirements on a locked device and parse through applications such as Whatsapp, Facebook, Twitter, LinkedIn, and Skype.[99] As technology advances and the types of information stored on a device become more complicated, the term "forensic search" will encompass a broader spectrum of potential access. The cases discussed below exemplify different perspectives on the level of intrusiveness exercised when law enforcement conducts a forensic search.

1. Forensically Intrusive

Under Ninth Circuit precedent, any digital forensic search at the border requires reasonable suspicion.[100] In *United States v. Cano*, border authorities conducted a download of a phone using Cellebrite software.[101] That software allowed agents to access several applications of choice, including text messages and call logs.[102] The agents could not, however, access third party applications like Facebook or WhatsApp.[103] Nonetheless, in the court's view, the agent's use of forensic technology required reasonable suspicion of illicit activity because they used forensic technology.[104]

2. Manually Intrusive

In contrast, the Eastern District of Michigan held that forensic technology that allows agents to view thumbnail previews of pictures and videos was less intrusive than a manual search.[105] It reasoned that a manual

98. Laura Nowell, *Privacy at the Border: Applying the Border Search Exception to Digital Searches at the United States Border*, 71 FED. COMM. L. J. 85, 93 (2018) (citing the National Criminal Justice Reference Services levels of invasive data extraction ranging from logical extraction, physical extraction, Chip-off extraction, and micro read extraction); SEAN E. GOODISON ET AL., DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM (2014).

99. Azimuddin Khan & Zakir Mansuri, *Comparative Study of Various Digital Forensics Logical Acquisition Tools for Android Smartphone's Internal Memory: A Case Study of Samsung Galaxy S5 and S6*, 9 INT'L J. OF ADVANCED RES. IN COMPUTER SCI. 357 (2018).

100. United States v. Cano, 934 F.3d 1002, 1016 (9th Cir. 2019) (citing United States v. Cotterman, 709 F.3d 952, 968 (9th Cir. 2013)).

101. *Id.* at 1008–09.

102. *Id.*

103. *Id.*

104. *Id.* at 1016.

105. United States v. Feiten, No. 15-20631, 2016 WL 894452, at *1, *6 (E.D. Mich. Mar. 9, 2016).

search may call for picture by picture, file by file review of data on a device, whereas a search conducted with forensic technology allows law enforcement to conduct a cursory search of thumbnail images.[106] Therefore, forensic technology permits law enforcement to pursue a less invasive and potentially less time-consuming electronic search than manual searches.

3. Temporally Intrusive

The United States District Court for the District of Massachusetts recently ruled on a case that also recognized manual searches can be more intrusive than forensic searches.[107] The court held that "even a basic search allows for both a general perusal and a particularized search of a traveler's personal data . . . ."[108] Therefore, instead of authorizing forensic searches that may be less intrusive, the court ruled that reasonable suspicion is required for any "non-cursory" electronic device search at the border.[109] According to the court, a cursory search is one that is long enough to determine "whether a device is owned by the person carrying it across the border, confirming that it is operational and that it contains data."[110] A search that takes any longer than necessary to conduct those tasks is non-cursory, requiring reasonable suspicion of illegal activity before it can be performed.[111]

Proponents of a warrant requirement for electronic data searches at the border agree that the distinction between forensic and manual searches is a false one.[112] Promoting this distinction only deprives the device owner and law enforcement of technology that could be used to save the time required to manually review digital data. As privacy advocates note, by demanding a higher level of suspicion for forensic searches than manual searches, courts set a line in the sand that does little to curb off searches of personal information.[113] The quick look standard ostensibly limits law enforcement intrusiveness on a temporal scale, but it lacks specificity and predictability. A far better solution would be for Congress to set an objective standard for digital device searches at the border. Legislation would not only help to avoid unpredictable standards but also prevent awkward judicially created tests.

106. *Id.* at *6.
107. Alasaad v. Nielsen, 419 F. Supp. 3d 142, 165 (Mass. Dist. Ct. 2019).
108. *Id.* at 163.
109. *Id.* at 173.
110. *Id.* at 163.
111. *Id.* at 169–70.
112. Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant-Appellant and Reversal, *supra* note 29, at 15.
113. *Id.* at 15–16.

C. When is a Border Search Not a Search Incident to Arrest?

The border exception is unique among Fourth Amendment exceptions because it was developed with sovereign interests in mind. Accordingly, the problem of contraband crossing the border in the digital age calls for unique technology, rather than comparisons to other exceptions. Nonetheless, such comparisons are ubiquitous. In *Riley v. California*, the Supreme Court rejected government authority to conduct cell phone searches incident to arrest.[114] This case is frequently cited in the context of any issue related to electronic device searches and Fourth Amendment exceptions.[115] While analogies can be drawn, they are limited because the Court's application of a Fourth Amendment exception in *Riley* is much different than the considerations assessed at the border.[116] *Riley* offers insight into the Court's stance on digital privacy, but its concerns with law enforcement's access to electronic data must be analyzed in a very different context when applied to the rationale for creating a border exception to the Fourth Amendment.

In August 2009, law enforcement stopped David Riley's vehicle after seeing that it had expired registration tags.[117] Ultimately, this observation led to an arrest for possession of a concealed and loaded firearm.[118] Two hours after his arrest, detectives from a gang unit searched Riley's phone and found evidence connecting him to a shooting.[119] In its analysis of law enforcement authority to search Riley's phone incident to his arrest, the Court noted the absence of "founding era" guidance from the Framers on how to address the threat of cell phone data.[120] Accordingly, it resorted to a balancing test that weighed the level of intrusion a cell phone search imposes on an individual's privacy against the "promotion of legitimate governmental interest."[121] The Court held that searches conducted, incident to an arrest, do not require a warrant supported by probable cause because there is a significant interest in officer safety and a need to "'disarm and discover evidence.'"[122] While not foreclosing the possibility that the phone itself could be used as a dangerous weapon, the Court concluded that the data on it was unlikely to present an imminent

---

114. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

115. *See, e.g.*, Thomas Mann Miller, *Digital Border Searches After Riley v. California*, 90 WASH. L. REV. 1943 (2015); Laura Nowell, *Privacy at the Border: Applying the Border Search Exception to Digital Searches at the United States Border*, 71 FED. COMM. L. J. 85, 94–98 (2018).

116. *Riley*, 134 S. Ct. at 2488.

117. *Id.* at 2480.

118. *Id.*

119. *Id.* at 2480–81.

120. *Id.* at 2484.

121. *Id.* (citing Wyoming v. Houghton*,* 526 U.S. 295, 300 (1999)).

122. *Id.* at 2484–85.

threat to law enforcement.[123] Accordingly, under the circumstances, the phone's data could not be searched without a warrant.[124]

In addition to the obvious distinctions between a search incident to arrest and the protection of sovereign interests at the border, two key differences stand out between *Riley* and borders search cases: (1) *Riley* did not address the degree to which the phones were examined, forensic or otherwise; and (2) in *Riley*, the government's concern was that evidence might be lost,[125] whereas in border cases, there is an expectation that the device owner has done what he or she can do to dispose of evidence. As they approach the border, travelers are prepared for inevitable inspection by law enforcement that will encroach upon at least some of their privacy. It stands to reason that a traveler anticipating search and inspection by border authorities are more likely to destroy, erase, or encrypt data they do not want law enforcement to examine.

Overall, while *Riley* recognizes the sanctity of a traveler's phone and the data contained in it, it does not balance privacy interests against sovereign interests to protect national security. Accordingly, recognizing the Supreme Court's concern for individual privacies under one Fourth Amendment exception does not guarantee that those interests override national security concerns in the border context. To prevent the Court from having to balance individual privacy and national security interests, Congress should set a standard that takes privacy and sovereign interests into account by using technology to identify adversarial threats. Legislation should recognize the distinction between routine searches and non-routine searches requiring prolonged detention. It should also recognize that border searches, like motor vehicle searches, are conducted to identify contraband and instrumentalities of a crime before a traveler makes way toward a place where they can use their cargo to harm others.[126] However, unlike other warrantless searches, the border search not only protects citizenry from contraband used to commit crimes but also protects national security interests by identifying threats that attempt to enter or depart the country.

D. Application to Vessel Searches

A much more apt analogy that emphasizes sovereign interests in border searches is demonstrated through the parallels between border

123. *Id.* at 2485.

124. *Id.* at 2495.

125. *Id.* at 2479, 2486–87.

126. *See* Carroll v. United States, 267 U.S. 132, 153 (1925) (holding that a warrant is not required to search mobile things like cars because they can be quickly moved out of the jurisdiction where a warrant might be obtained). *But see* Maryland v. Dyson, 527 U.S. 465, 466–67 (holding that a vehicle search must be supported by probable cause that the vehicle contains contraband, but a separate exigency requirement is not a prerequisite to a warrantless vehicle search).

search authority and vessel search authority. In *United States v. Villamonte-Marquez,* the Supreme Court held that a warrantless search of a vessel is valid because waterborne commerce is distinct.[127] "[A]ccess to the open sea" and the "impressive historical pedigree" of warrantless searches aboard vessels call for a unique exception to Fourth Amendment requirements.[128] Similarly, border search authority gives special dispensation to rare opportunities to syphon out evidence of illicit activity. Border search authority and vessel search authority are based, in part, on the premise that law enforcement needs to ensure compliance with importation laws and pursue a tax on goods and material where appropriate.[129] However, there is a long-held recognition that vessel searches may reveal other types of illicit activity.[130]

As microchip storage and processing speeds develop, individuals crossing the border have an increased ability to carry large amounts of sensitive information.[131] Accordingly, the parallel between the exception for vessel searches and the warrant exception for border searches is closer today than it was at its inception. In addition to the massive amount of cargo these ships carry, they also arrive in and depart from ports in the United States with incredible amounts of data on the ship's server.[132] Therefore, commercial ships entering and departing from ports offer a macro view of border search authority.

Looking at the true purpose of the Fourth Amendment exception for border searches and vessel searches may reveal that the two exceptions have far more in common than a border search and a search incident to arrest. Vessel searches and border searches both establish authority for customs officials to seize onto fleeting opportunities to catch nefarious deeds as they cross the threshold of U.S. sovereignty by inspecting cargo and belongings. Restrictions to the "impressive historical pedigree," that established an exception to the warrant requirement in circumstances where people and their belongings are moving between jurisdictions and sovereign territories, should be levied by unified federal law rather than a disjointed court system.

---

127. United States v. Villamonte-Marquez, 462 U.S. 579, 592–93 (1983).

128. *Id.*

129. *See* PETER ANDREAS, SMUGGLER NATION: HOW ILLICIT TRADE MADE AMERICA, 78–79 (2013) (discussing the founding era struggle to enforce embargoes and importation laws through customs search authority while building a strong economy).

130. *See* United States v. Varlack Ventures, Inc., 149 F.3d 212, 218 (3d Cir. 1998) (reversing a district court order to suppress evidence of oil pollution obtained from the vessel *Venture Pride*).

131. *See* Miller, *supra* note 115, at 1969, 1996.

132. *See* Jill Connors, *Counting Your Megabytes – From the Middle of the Ocean*, KVH (May 2, 2012), https://www.kvhmobileworld.kvh.com/counting-your-megabytes-from-the-middle-of-the-ocean/ [https://perma.cc/G5G5-E8RU].

The judiciary's attempt to rationalize limitations to border search authority has resulted in precedent that lacks congruity with how law enforcement actually conducts electronic device searches at the border. Vessel search authority is evidence that there is precedential importance in retaining law enforcement's ability to conduct suspicionless searches in circumstances where threats can rapidly escape law enforcement interdiction. To preserve and improve upon these authorities in the information age, Congress should enact legislation that counters the ability to conceal evidence of a national security threat. That legislation should take into account the significance of the border demarking sovereign boundaries and expectations of privacy. Legislation can take both concerns into account by using technology to objectively identify threats on phones and other portable devices.

III. HOW CAN CONGRESS PREVENT THREATS WITHOUT BORDER OFFICIALS INTRUDING ON PRIVACY?

Judges and advocates alike are eager for legislation to resolve law enforcement's responsibility for intercepting and searching digital media crossing the border.[133] A statute will set a standard that can be appreciated by courts and the public. It will also presumably reflect the reality of technological capabilities that exist by considering both the threats and expectations of the average citizen.

Recognizing an unquestionable divide between how courts and the average American view their privacy rights at the border, Congress has attempted to find solutions through legislation. One proposal, advanced by Senators Ron Wyden and Rand Paul, would authorize suspicionless forensic searches at the border for non-U.S. persons but would require a finding of probable cause and issuance of a warrant before viewing electronic media possessed by any U.S. person.[134] This proposal suffers from two notable deficiencies. First, by eliminating the Fourth Amendment border exception for U.S. persons, the bill ignores a significant portion of potential threats because it requires a stronger basis for searching the belongings of U.S. citizens, like Ali Saboonchi, who pose a threat to national security. Second, it assumes that by allowing searches of a foreigner's data, a U.S. citizen's data will somehow be protected. Undoubtedly, there is a high probability that U.S. person's data would exist

133. *See*, *e.g.*, Abidor v. Napolitano, 990 F. Supp. 2d 260, 274 (E.D.N.Y. 2013) (recognizing efforts to circumscribe electronic data searches in the absence of legislation); S. 2462, 115th Cong. (2018); Adam Schwartz & Sophia Cope, *Pass the Protecting Data at the Border Act*, ELECTRONIC FRONTIER FOUND. (Oct. 13, 2017), https://www.eff.org/deeplinks/2017/10/pass-protecting-data-border-act [https://perma.cc/7ADE-UVGN].

134. Protecting Data at the Border Act, S. 823, 115th Cong. (2017).

on an electronic device carried by a foreigner entering or departing the United States.

Other legislation, including bills setting temporal parameters for Customs holding an electronic device[135] or requirements for the Department of Homeland Security to implement regulations on electronic device searches at the border,[136] have not passed through both houses of Congress. Ultimately, Congress's current proposed solutions fail to secure U.S. citizen's data while simultaneously impeding law enforcement's ability to access a significant amount of data that presents national security concerns.

A solution, that would directly address the struggle between a traveler's desire to guard personal information contained in electronic devices and the concern that border enforcement are not exercising constitutional authority to search data that crosses the border, would recognize both values. Congress, in its discretion, should place reasonable restraints on border searches to protect the public's privacy interests. However, just as law enforcement should be held to a stricter standard than an "anything goes" approach when searching a traveler's device,[137] border officials should not be required to seek out a warrant when the data stored in a traveler's device can be of significant concern to sovereign interests. The border search exception to the warrant requirement was carefully tailored to address threats to U.S. interests. Accordingly, restrictions to that exception should also be carefully tailored with more meaningful specificity than a simple distinction between manual and forensic searches.

A. Limiting Searches to Particular Types of Data

Privacy expectations in an individual's home "are most heightened."[138] Therefore, one bright-line rule that Congress should impose is to prohibit suspicionless searches of cellphone applications that access information that is protected in the home. Cellphone applications that access in-home security cameras are just one example of that kind of information.[139] Another sensible limitation is to restrict access to data stored

135. Securing Our Borders and Our Data Act, H.R. 239, 111th Cong. (2009).

136. Border Security Search and Accountability Act of 2009, H.R. 1726, 111th Cong. (2009).

137. *See* United States v. Seljan, 547 F.3d 993, 1000 (9th Cir. 2008) (rejecting an argument by the government that its discretion to search personal effects at the border is so broad that "anything goes").

138. *See*, *e.g.*, Kyllo v. United States, 533 U.S. 27, 33 (2001) (citing Dow Chemical v. United States, 476 U.S. 227, 234, n. 4 (1986)).

139. In *Kyllo v. United States*, the Supreme Court established the principle that law enforcement cannot use technology as a means of subverting Constitutional protections. 533 U.S. 27, 32 (2001). In that case, the Court held it is unlawful to search a house without a warrant using thermal imaging technology. *Id.* at 40.

on some distant server.[140] Though not constitutionally required in all instances, Congress exercises its proper role by implementing such limitations that restrict border searches of personally held electronic information while ensuring that law enforcement can effectively identify threats to national security.

Limited access to Global Positioning Systems data might be appropriate in circumstances where law enforcement does not possess a warrant. Recent locations may be informative to law enforcement in establishing the traveler's intentions for crossing the border. If law enforcement has information regarding the location of particular threats to national security, it should be applied through forensic technology to identify travelers that pose a risk to the country. One example might be an instance where law enforcement obtains information that a house is known to store weapons transported across the border. In that case, law enforcement should be able to use information regarding known national security concerns to identify weapons illegally crossing the border. Such restraints and authorizations are in line with the exception because they limit the scope of law enforcement's search to the information and activity before them at the border. To prevent uneven application of the border exception, Congress should enact legislation that not only sets an explicit standard for suspicionless searches at the border but also leverages technology to provide law enforcement with the tools needed to protect border interests while also maximizing personal privacy concerns.

B. Using Artificial Intelligence to Syphon Out Serious Threats

Artificial intelligence (AI) has proven valuable for law enforcement in terms of identifying particularly concerning threats and targeting higher-level criminals, like drug dealers, instead of individuals possessing small quantities of illegal narcotics.[141] Using image and text classifiers, law enforcement would be able to expose networks attempting to smuggle information like the type Ali Saboonchi had on his devices.[142] Recently, the messaging software platform WhatsApp blocked 130,000 accounts used for child pornography with the assistance of AI.[143] By specifically tailoring search criteria to the most serious national security threats, law enforcement

---

Similarly, it stands to reason that law enforcement could not use technology on someone's phone to look into their house.

140. *See* CBP DIRECTIVE NO: 3340-049A, *supra* note 52.

141. *See*, *e.g.*, Patrick H. O'Neil*, How Police Use AI to Hunt Drug Dealers on Instagram*, DAILY DOT (May 10, 2016, 2:05 PM), https://www.dailydot.com/layer8/instagram-drug-dealing-attorney-general/ [https://perma.cc/H245-2H9X].

142. *Id.*

143. *130000 WhatsApp Accounts Blocked . . . Never Do This*, NEWS24ONLINE (Jan. 10, 2019), https://news24online.com/news/130000-whatsapp-accounts-blockednever-do-9ac39d0a/ [https://perma.cc/66KS-JAR9].

would be able to focus their efforts while easing concerns of bias and incidental exposure of personal information. Congress could require such initiatives and promote projects that incorporate AI projects into agency regulation.

Daniel Wietzer, a leading scientist in artificial intelligence research, was recently quoted as saying, "I hope the policymakers come away with a clear sense that AI technology is not some immovable object, but rather that the right interaction between computer science, government, and society at large will help shape the development of new technology to address society's needs."[144] Congress is looking at ways to use AI that will improve the economy.[145] While those opportunities are evolving, the technology that is available today should be used to protect existing resources and filter out active threats. Using existing technology, Congress should support border search authority, and also protect personal information that does not threaten national security, by encouraging agencies to engage in forensic examinations with programs that minimize officer discretion and exposure to electronic files while identifying evidence of sanctions violations and other dangerous data.

1. Artificial Intelligence Development

AI represents a solution to some and a feared civil intrusion to others. Given recent triumphs by WhatsApp and law enforcement using this technology, it is evident that AI is the most successful when it is targeted and monitored for effectiveness. National security can be improved by harnessing the benefits of programming advancements that can identify the most concerning threats like information concerning the transfer of arms technology, while protecting civil liberties through effective oversight and regulation.[146]

Artificial intelligence has been defined as an activity devoted to enabling machines to function appropriately and with foresight in their environment.[147] In the context of digital device searches, AI would be used to survey a broad assortment of file formats including emails (i.e. EML or

144. Peter Dizikes, *AI, The Law, and Our Future*, MIT NEWS (Jan. 18, 2019), http://news.mit.edu/2019/first-ai-policy-congress-0118 [https://perma.cc/9SRH-RKBW].

145. National Artificial Intelligence Initiative Act of 2020, H.R. 6216, 116th Cong. (2020).

146. While AI is the focus of several new technological developments, it has been in development for nearly a century and is credited with allied successes over Germany in World War II. *See* Viraj T, *Encapsulating the Entire Evolution of Artificial Intelligence*, AITHORITY (June 7, 2019), https://aithority.com/ait-featured-posts/the-evolution-of-artificial-intelligence/ [https://perma.cc/X5ZN-355Y].

147. PETER STONE ET AL., ARTIFICIAL INTELLIGENCE AND LIFE IN 2030 12 (2016), http://ai100.stanford.edu/2016-report [https://perma.cc/S688-KCF3].

MSG files), pictures (i.e. JPEG, TIFF, or GIF files), and documents (i.e. DOC, PDF, EXL files), but it would require continual input from government intelligence entities to identify the threats that are the most concerning. With that input, AI forensic programing would continually learn by identifying evolving data patterns that trace back to threats identified by intelligence analysts.

2. Whose Device is Subject to Screening?

The Honorable Judge Grimm and others have noted that law enforcement resources are limited in their ability to regularly conduct either "random or suspicionless forensic searches."[148] However, devices may be appropriately identified for screening by targeting threats in manageable batches, whether that means identifying large groups for screening (i.e. all devices on a single cruise ship in a port or a single airplane in an airport), algorithmically identifying random devices subject to screening, or some combination of the two methods.[149] Whatever method might be used to select devices, regulatory entities must recognize most methodologies will have an inherent bias that should be continually monitored and refined to prevent civil liberty violations.

3. How Can AI Help?

Once a manageable set of electronic devices are selected using a process similar to one of those mentioned above, border officials would access the device using analytical software. Access to encrypted devices and software continues to be an ongoing issue. Some have suggested that encryption might be broken with quantum computing, a super computer technology that can analyze several calculations simultaneously.[150] However, even if an encryption-breaking computer is invented, it is likely that more secure encryption can be created.[151] Accordingly, the government's best answer to breaking encryption might be to entice

148. United States v. Saboonchi, 990 F. Supp. 2d 536, 570 (D. Md. 2014) (citing United States v. Chaudhry, 424 F.3d 1051, 1054 (9th Cir. 2005)).

149. *See* STONE ET AL., *supra* note 147, at 29, 35.

150. *See* Dorothy E. Denning, *Is Quantum Computing a Cybersecurity Threat?*, AM. SCIENTIST (Mar./Apr. 2019), https://search.proquest.com/openview/3876c9eebe4c7ebf38c3b180b521ed09/1?pq-origsite=gscholar&cbl=40798 [https://perma.cc/C3PQ-KVKA].

151. *See* Emerging Technology from the arXiv, *How a quantum computer could break 2048-bit RSA encryption in 8 hours*, MIT TECH. REV. (May 30, 2019), https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/ [https://perma.cc/B5SC-QNJA].

technology manufacturers to identify ways of bypassing the encryption they create.[152]

After gaining access to devices, law enforcement would use analytical software to survey data on the devices for threats. These threats might be presented in the form of communications that discuss planning organized attacks, or in the form of other concerning anomalies in data that is available on the device.[153] Insider threat programs used by businesses and government agencies have successfully analyzed big data and identified concerning behavior.[154] Similar programming should be developed to analyze devices crossing a port of entry to limit personal biases that may target a device or its owner for improper reasons.

C. Legislating AI-Driven Searches at the Border

There is no doubt that AI will transform society in the coming decades. Since 2016, the number of organizations lobbying artificial intelligence issues has grown more than nine-fold.[155] In response to this growing trend, Congress is integrating AI regulation into its legislation.[156] As it does so, it should also use AI to create opportunities for the government to compete in the technological domain.

---

152. The EARN IT Act of 2020 and similar legislation may create an incentive for service providers to make decryption techniques more streamlined and predictable. *See* Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020, S. 3398, 116th Cong. (2020).

153. Behavior-Based Access Control systems are programs that analyze large sets of data including text messages, chats, and computer files to assess whether there is a pattern that is consistent with threatening behavior. MICHAEL MAYHEW ET AL., USE OF MACHINE LEARNING IN BIG DATA ANALYTICS FOR INSIDER THREAT DETECTION 2–3 (2015).

154. Lynh Bui et al., *Lieutenant's Use of Work Computer Alerted Coast Guard to His Terror Plot, Authorities Say*, L.A. TIMES (Feb. 22, 2019, 9:50 AM), https://www.latimes.com/nation/la-na-us-coast-guard-christopher-hasson-terrorist-attack-20190222-story.html [https://perma.cc/6MNW-F67N].

155. Gopal Ratnam & Kate Ackley, *Artificial Intelligence is Coming. Will Congress Be Ready?*, ROLLCALL.COM (June 10, 2019, 7:00 AM), https://www.rollcall.com/news/artificial-intelligence-congress-ready [https://perma.cc/8ZRX-ZMDS].

156. The Library of Congress found that the 115th Congress referenced AI in thirty-nine bills, four of which have been enacted into law. *See* Eduardo Soares et al., *Regulation of Artificial Intelligence: The Americas and the Caribbean*, LIBRARY OF CONGRESS (Jan. 2019), https://www.loc.gov/law/help/artificial-intelligence/americas.php [https://perma.cc/K9N3-7F53].

1. Components of a Legislative Solution

One statute defines AI as having five components, but it is basically described as computing software that aids in decision-making processes without significant human input.[157] It has a broad spectrum of application which can be broken down into three types of tasks: (1) "machine learning (computers using data to make predictions);" (2) "natural-language processing (computers processing and understanding a natural human language like English);" and (3) "computer vision or image recognition (computers processing, identifying, and categorizing images based on their content)."[158]

In a forensic search, machine learning and computer image recognition software should be used to identify data that is most likely to trigger a national security concern. In the case involving data on Ali Saboonchi's electronic devices, forensic software would compile a number of factors including the names of equipment Saboonchi shipped; Iranian websites and email addresses stored on the device; and connections with U.S. manufacturers that sell goods that may not be shipped to Iran under sanction laws. Computer image recognition should also be used to identify images that may trigger particular concerns. While no single factor would be determinative, each of the above factors, including the names of sanctioned equipment, would collectively help identify suspicious data on a device. AI review would also be conducted with programing designed to minimize unwanted bias by deselecting terms that target free speech, religion, or minorities. For instance, a specifically named technology, like a thermocouple, requiring a trade license might factor into concerns with a device, but the software would eliminate from consideration the name of a religious group that happens to be prominent in a country subject to U.S.

157. The John S. McCain National Defense Authorization Act of 2019 defines AI as including: (1) any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets; (2) an artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action; (3) an artificial system designed to think or act like a human, including cognitive architectures and neural networks; (4) a set of techniques, including machine learning that is designed to approximate a cognitive task; and (5) an artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting. *Id*. (citing The John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 115th Cong. (Aug. 13, 2018)).

158. Jennifer Betts, *Keeping an Eye on Artificial Intelligence Regulation and Legislation*, NAT'L L. REV. (June 14, 2019), https://www.natlawreview.com/article/keeping-eye-artificial-intelligence-regulation-and-legislation [https://perma.cc/L5L3-Z44K].

sanctions. The AI program would also be further refined with continual modification to remove unwanted bias that may develop as targeted data sets build historical context.

One of the primary objections to AI, especially in the law enforcement context, is that it is based on data that may be tainted by existing human biases.[159] High volume, diverse, data sets, and vigilant result monitoring will help address this concern.[160] International airports and other ports of entry are an ideal place to obtain high volume, diverse, data sets that can be monitored to adjust AI results.

To minimize bias and continually improve on an AI solution, legislation should require a forensic analysis process that includes five components: (1) research to identify the best algorithms for identifying national security threats on a device while limiting law enforcement access to private information; (2) a pilot program to test forensic software's ability to identify concerning data on devices entering or departing the country; (3) phased-in AI implementation with continual improvement; (4) a thorough oversight program; and (5) unique and specialized auditing to ensure civil liberties are being protected when AI is used to identify threats on devices.

In the research phase, Department of Homeland Security forensic labs will work with the National Institute of Standards and Technology and other forensics experts to develop software that can identify terms and images that are key indicators of criminal activity presenting a national security concern. Information gathered from electronic devices seized in past law enforcement efforts may be used to create a program that learns the most common traits in targeted criminal activity.

Once a satisfactory program is designed, a pilot program should be implemented in a high-density port of entry. The port of entry should have a diverse demographic so that the software can be thoroughly tested for bias. The pilot program should be specifically tested to minimize bias and search for the objective criteria that seeks out national security threats without relying on prejudicial data.[161] Objective criteria must be identified for determining which devices will be searched. Border officials would identify devices that are subject to forensic review either through an algorithm that

---

159. Randy Rieland, *Artificial Intelligence is Now Used to Predict Crime. But Is It Biased?*, SMITHSONIAN.COM (Mar. 5, 2018), https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/ [https://perma.cc/RQN7-XQEL].

160. Craig S. Smith, *Dealing with Bias in Artificial Intelligence*, N.Y. TIMES (Nov. 19, 2019), https://www.nytimes.com/2019/11/19/technology/artificial-intelligence-bias.htm [https://perma.cc/Z2KX-LPUS].

161. One example of prejudicial data is a zip code that is common amongst individuals that border authorities may seek to prevent from entering the country. Distinguishing threats by zip code is one example of inappropriate bias because it may inappropriately identify a threat merely by identifying members of an economic class rather than by factors that present a causal link to identified threats.

incorporates random selection criteria or, as discussed above, when a selection algorithm is impractical, officials should select a particular sample group. For instance, officials could set parameters on the number of devices searched by randomly selecting one airplane in an airport and requiring a search of all devices on that plane.

In phase three, the program is incorporated into standard use at the border, while continually being improved. As the forensic software is implemented at the border, it will inevitably identify new patterns that it finds common among travelers that pose a national security threat. Program overseers will need to make adjustments to the algorithm and improve it to ensure it is serving the intended purpose without undue bias. If border authorities wish to retain information obtained from portable devices, there should be transparent procedures in place. Legislation should mandate regulations identifying the type of information that will be retained and the circumstances that warrant retention.

Phase four establishes a continual oversight program. Congress is developing a structure for overseeing artificial intelligence in the private sector.[162] A similarly designed government oversight program will help Congress find the best methodologies for protecting personal information when programs use AI. In implementing both private and public sector AI oversight, Congress should standardize mechanisms to the greatest extent possible so that common issues and improvements can be understood from other AI uses.

The last component of a Congressionally implemented AI program for vetting devices at the border will involve a specialized audit. Inspectors General are creating programs to improve AI oversight.[163] AI software used in forensic tools at the border should be overseen using similar programs, but it must be designed with specificity to address the massive quantity of information that would be gathered at the border. Auditing initiatives must also be designed to oversee AI programs that are continually adapting to minimize bias.

2. Draft Legislation

Some members of Congress have recognized that current border search policy for identifying threats contained on digital devices is inadequate. As a result, advanced, well-reasoned legislation that ensures proper handling of privileged material and limits the number of days to

---

162. *See* Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (Apr. 4, 2019).

163. Andrew Eversden, *Here's How a National Intelligence Watchdog is Improving AI Oversight*, C4ISRNET (Nov. 26, 2019), https://www.c4isrnet.com/artificial-intelligence/2019/11/26/heres-how-a-national-intelligence-watchdog-is-improving-ai-oversight/ [https://perma.cc/3YVQ-SX82].

decrypt and exploit a device has been introduced.[164] Many aspects of that legislation should be adopted, but it should also be further developed to clarify that suspicionless searches may be conducted at the border when executed in a reasonable manner. The following draft legislation should be added to existing legislative proposals to set a standard for reasonable searches:[165]

A BILL

To protect U.S. interests by requiring the Secretary of Homeland Security to implement the use of algorithmic software to search electronic devices.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress Assembled,

SEC. 1. SHORT TITLE.

This Act may be cited as the "Electronic Device Search Act of 2020."

SEC. 2. ELECTRONIC DEVICE SEARCHES OCCURRING AT THE BORDER.

(a) IN GENERAL. – This Act confirms the constitutional authority of authorized agents to search electronic devices entering or departing the U.S. through a designated port of entry.

(b) ELECTRONIC DATA EXTRACTION AND ANALYSIS. – To the maximum extent possible, algorithmic software shall be developed to limit bias in determining what devices are searched while identifying data that presents the greatest threats to U.S. interests. Data extraction technology shall be developed and used to analyze electronic devices crossing the U.S. border.

164. Border Security Search Accountability Act, H.R. 1726, 111th Cong. (2009); Securing Our Borders and Our Data Act, H.R. 239, 111th Cong. (2009).

165. The Securing Our Borders and Our Data Act, H.R. 1726, 111th Cong. (2009) is a good template for policy to advance personal privacy interests, but this bill should be amended and supplemented to add provisions that advance national security interests while also furthering personal privacy interests.

SEC. 3. IMPLEMENTING A RULE WITH RESPECT TO BORDER SECURITY SEARCHES OF ELECTRONIC DEVICES.

(a) REGULATIONS. – Not later than 180 days after the date of the enactment of this Act, the Secretary, acting through the Commissioner of the United States Customs and Border Protection, in coordination with the Assistant Secretary of Homeland Security for United States Immigration and Customs Enforcement and the senior official appointed pursuant to section 222 of the Homeland Security Act of 2002 (6 U.S.C. § 142), shall issue a rule with respect to the scope and procedural recordkeeping requirements associated with border security searches of electronic devices.

(b) CONTENT. – The rule issued pursuant to subsection (a) shall include the following:

(1) A requirement that electronic device searches shall be conducted by only accessing data available on the device itself. The requirement shall ensure that information is not collected through internet connectivity or other means that would access databases separate and distinct from those on the device itself.

(2) A requirement that limits access to location information such that location information is only analyzed to the extent necessary to confirm the intended purpose for a traveler crossing the border.

SEC. 4. ELECTRONIC DEVICE SEARCH PROGRAM.

(a) IN GENERAL. – The Secretary shall implement a program applying technological developments to limit opportunities for bias in conducting electronic device searches. At a minimum, the Program shall be composed of four phases:

(1) RESEARCH. – In coordination with the Department of Justice, the Secretary shall establish a Memorandum of Understanding with the National Institute of Standards and Technology to develop capabilities for searching electronic devices to identify data presenting a threat to U.S. interests. The capabilities developed should identify both digital images and digital text in multiple formats that may present a concern to U.S. interests.

(2) PILOT PROGRAM. Not later than two years after the enactment of this Act, the Secretary shall establish a pilot program using electronic device search capabilities developed in subsection (a)(1). The program shall be implemented in at least two high-density ports of entry and identify objective criteria for determining which devices are searched. The program shall be specifically designed to assess device selection bias, device search bias, and methods to limit bias.

(3) PHASED-IN IMPLEMENTATION. Not later than three years after enactment of this Act, the Secretary shall establish criteria and a timeline for implementing electronic device search capabilities in all ports of entry.

(4) OVERSIGHT AND IMPROVEMENT. The Secretary shall identify methods for ensuring that the electronic device search program continually improves to both identify evolving threats to U.S. interests and limit bias.

(b) AUDITING. – The Secretary, acting through the Inspector General of the Department of Homeland Security, shall develop a specialized auditing program designed to review methods for identifying electronic device selection and electronic device search bias. Auditors shall be familiar with algorithms and programing software used to search electronic devices at the border.

***

As discussed above, encryption techniques make it increasingly difficult for law enforcement to access phones and devices.[166] Absent legislation that creates mechanisms for law enforcement to access encrypted data, there is no easy solution to this problem. In order to take the necessary time to assess the risk of devices crossing the border, allowances must be made for forensic analysts. Travelers that do not authorize forensic scans of their phones may experience delays, but legislation should create mechanisms to ensure that law enforcement acts with due diligence to return devices to their owners. If a device or information on it is encrypted with software that prevents access, officials should be allowed to hold the device for at least twenty-four hours to attempt decryption. If significant data is inaccessible to the AI software, absent probable cause, the

166. Perlroth, *supra* note 43.

opportunity to search it will be foregone until forensic technology improves.

CONCLUSION

Expectations of privacy at the border must keep pace with the times and so too must Congress. Well-crafted solutions will use technology to promote privacy and security interests simultaneously. The border exception has a long history of protecting sovereign interests by catching national security concerns before they cross the border. That important precedent should not be eroded because technology has advanced. Instead of creating new standards that reduce law enforcement's access to information at the border, lawful and well-thought through technology applications should be used to counterbalance technology that is used to conceal evidence of illegal conduct. Congress should enact legislation that requires border authorities to use artificial intelligence programming to identify threats. This technology should be continuously vetted to cull out bias and minimize privacy intrusions.

Inevitably, there will be cases where data that is harmful to national security interests evades border authorities. As the prospective volume of that data increases with technological advances, so does the opportunity for increased risks. In response, law enforcement should be equipped to unveil threats without imposing undue burdens on personal rights. Congress needs to help law enforcement by implementing legislation that will allow border officials to adapt their law enforcement techniques before constitutional law administration tactics are sacrificed and civil liberties are made vulnerable to national security threats that seep through the border.