BACK TO THE FUTURE OF YOUR LAPTOP:
HOW BACKLASH OVER PROLONGED DETENTION OF DIGITAL DEVICES IN BORDER SEARCHES IS SYMPTOMATIC OF A NEED FOR "REASONABLE SUSPICION" IN ALL BORDER SEARCHES OF DIGITIAL DEVICES

TOM RECHTIN*

Table of Contents

* Dr. Thomas Rechtin earned his PhD in English from Binghamton University in 2004. He has taught English at Binghamton University, Slippery Rock University, and Misericordia University, and he is also a published poet in magazine and chapbook form. He is currently in his third year of studies at Ave Maria School of Law in Naples, Florida where he is interning for federal magistrate Judge Douglas N. Frazier of the Middle District of Florida. He plans to practice law in Florida.

ABSTRACT

On March 8, 2013, the Ninth Circuit in *U.S. v. Cotterman* held that, in order to conduct a forensic examination of a digital device at the border, one must possess a "reasonable suspicion" that a crime was being committed.[1] In so holding, the *Cotterman* court emphasized the privacy rights at stake in such a potentially invasive search into the personal contents of one's digital device. And yet, the *Cotterman* court, like courts before it, failed to recognize a more fundamental justification for a heightened level of suspicion in border searches of digital devices: namely, that the contents and capabilities of a digital device (such as a laptop computer) are sufficiently distinct in nature from their "real world" counterparts such as handbags and briefcases. The internet, for example, is a realm distinct in nature and kind from our external world, such that when a border search is effectuated of a device that permits access to such a realm, the search is no longer taking place solely at the physical border and of the physical digital device at said border. Rather, the search is also taking place in a "digital realm", thereby removing the search, in part, from the border and, accordingly, from the need for the sovereign to protect itself from outside threats. As a consequence, this bifurcated "reality" surrounding border searches of digital devices warrants a "reasonable suspicion" standard to honor both the search that is taking place at the border and the search that is not, while such a standard applies not just to those instances when a forensic examination of the digital device is conducted, but in all searches of such digital devices.

INTRODUCTION

Imagine yourself returning to the United States from a business trip in Hong Kong, an academic conference in Rome, or even a family vacation in picturesque Costa Rica. You arrive without incident at JFK in New York, deboard, and proceed towards customs, fingers crossed that you won't have to endure the inconvenience of your luggage being thoroughly searched. Unfortunately, this isn't your lucky day: customs pulls you aside and begins to unceremoniously rummage through your personal effects, amongst which is your trusty laptop computer, without which you practically go nowhere. To your surprise, the customs official asks you to turn on the laptop and provide your password. You hesitate, thinking of everything you've ever written, downloaded, or emailed in that computer, not to mention every website you've ever visited. But, as the official impatiently glares at you, you quickly realize you're in no position to bargain. So, you type in your password, and the customs official begins to scroll here and click there. After several uncomfortable minutes, the customs official finally closes the laptop and informs you that you are free to go . . . but the laptop must be detained for further analysis.

In *U.S. v. Cotterman*,[2] the Ninth Circuit Court of Appeals was confronted with just such a scenario when the court considered whether the border search of a laptop computer that ended two days later in a government lab 170 miles from the border still fell within the border search doctrine and thereby did not require any level of suspicion to be effectuated.[3] In the decision below, the district court did not see the removed nature of this search (both in terms of time and space) as the typical border-search situation and consequently granted the defendant's motion to

[1] U.S. v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013).
[2] U.S. v. Cotterman, 637 F.3d 1068 (9th Cir. 2011).
[3] *Id.* at 1070.

suppress the evidence seized from the laptop[4] because "the law requires the Government to have reasonable suspicion before extending the search in both distance and time away from the border."[5] However, the Ninth Circuit reversed the district court, rejecting that court's characterization of the search as an extended border search: "We find no basis under the law to distinguish the border search power merely because logic and practicality may require some property presented for entry—and not yet admitted or released from the sovereign's control—to be transported to a secondary site for adequate inspection."[6] In so rejecting the district court's analysis, the Ninth Circuit explicitly noted that it was not ascribing to an "anything goes" doctrine regarding searches at the border:[7] "The Government cannot simply seize property under its border search power and hold it for weeks, months, or years on a whim."[8]

Despite the Ninth Circuit's caveat on the federal government's ability to detain traveler's digital devices for prolonged periods of time, evidence is mounting that such detentions often occur for much longer than the two days in *Cotterman*[9] and, as a consequence, have many calling into doubt the reasonableness of such searches.[10] Of course, detentions of digital devices for weeks if not months is not necessarily incongruous to the Ninth Circuit's position, for the key consideration appears to be whether the federal government detained the laptop or other digital device "on a whim."[11] Indeed, in 2009 the federal government embraced just such a perspective when it issued two policies from the U.S. Customs and Border Protection[12] and U.S. Immigration and Customs Enforcement respectively,[13] both of which place no definitive time limitation on the government's ability to detain a laptop or digitial device to conduct a border search so long as it

---

[4] U.S. v. Cotterman, No. CR 07-1207-TUC-RCC, 2009 WL 465028, at *10 (D. Ariz. Feb. 24, 2009).

[5] *Id.* at *4.

[6] *Cotterman*, 637 F.3d at 1070 ("The border search doctrine is not so rigid as to require the United States to equip every entry point—no matter how desolate or infrequently traveled—with inspectors and sophisticated forensic equipment capable of searching whatever property an individual may wish to bring within our borders or be otherwise precluded from exercising its right to protect our nation absent some heightened suspicion." *Id.*). However, after granting a re-hearing, the Ninth Circuit clarified its position regarding searches of digital devices at the border. U.S. v. Cotterman, 709 F.3d 952 (9th Cir. 2013) [hereinafter *Cotterman (2013)*]. While affirming its position that searches of digital devices removed from the border both in terms of location and duration do not necessitate reasonable suspicion, *Id.* at 961-62, the court held that "reasonable suspicion was required for the forensic examination of [the defendant's] laptop." *Id.* at 957. The significance of this holding will be addressed at the conclusion of this note. *See infra* pp. 39-40 and accompanying notes.

[7] *Cotterman*, 637 F.3d at 1070.

[8] *Id.* ("[W]e continue to scrutinize searches and seizures effectuated under the longstanding border search power on a case-by-case basis to determine whether the manner of the search and seizure was so egregious as to render it unreasonable.").

[9] For example, in a 2010 search at the border, Pascal Abidor had his laptop detained for eleven days, while in 2010 David House also had his laptop, camera, and USB drive held by government officials for seven weeks pursuant to a border search. Susan Stellin, *Border Agents' Power to Search Devices Is Facing Increasing Challenges in Court,* N.Y. TIMES (Dec. 3, 2012), http://www.nytimes.com/2012/12/04/business/court-cases-challenge-border-searches-of-laptops-and-phones.html?pagewanted=all&_r=0.

[10] *See, e.g.*, Glenn Greenwald, *U.S. Filmmaker Repaetedly Detained at Border*, SALON (April 8, 2012), http://www.salon.com/2012/04/08/u_s_filmmaker_repeatedly_detained_at_border/.

[11] *Cotterman*, 637 F.3d at 1070.

[12] U.S. CUSTOMS AND BORDER PROTECTION, BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION, CBP DIRECTIVE NO. 3340-049 (2009) [hereinafter 2009 CBP DIRECTIVE], *available at* http://www.dhs.gov/xlibrary/assets/cbp_ directive_3340-049.pdf.

[13] U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, BORDER SEARCHES OF ELECTRONIC DEVICES, ICE DIRECTIVE NO. 9-6.1 (2009) [hereinafter 2009 ICE DIRECTIVE], *available at* http://www.dhs.gov/xlibrary/assets/ice_ border_search_electronic_devices.pdf.

is accomplished within a "reasonable" time.[14] Nevertheless, criticism from such groups as the ACLU has been levied against this governmental practice of seizing one's laptop or digital device in a border crossing without suspicion and for days if not weeks at a time.[15]

This note will argue that, while federal policy and recent appellate court decisions are a sensible response to the practical difficulties of adequately conducting searches of laptop computers and digital devices, the prolonged detention of such digital devices without suspicion in a border search is nevertheless unreasonable in its breadth and stems from a more fundamental misconception of the laptops and digital devices under governmental scrutiny at our borders. Indeed, prior to the current controversy over the suspicionless, prolonged detention of laptops and digital devices in border searches, courts were confronted with the more basic question of whether border searches of laptops and other digital devices (without being removed in time or space from said border) require reasonable suspicion. While the Supreme Court has yet to rule on the issue, circuit courts of appeals consistently held that no such reasonable suspicion was required.[16] In so doing, these courts rejected a variety of arguments in favor of the reasonable suspicion standard, many of which focused upon the seemingly unique status of the laptop or other digital device.[17] However, all parties involved failed to take into consideration the unique spatio-temporal position of the laptop and other digital devices with regards to the spatio-temporal position of the border search being effectuated against the laptop or other digital device. Indeed, as the requirement for no standard of suspicion to conduct routine border searches stems from a spatio-temporal event (the crossing of the border), it only makes sense that border searches of any devices that assert their own unique spatio-temporal dimensions[18] ought to operate under a heightened standard. After all—so the argument goes—while the border

---

[14] 2009 CBP DIRECTIVE at 5.3.1 Detention and Review by CBP p. 4 ("An Officer may detain electronic devices . . . for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible."); 2009 ICE DIRECTIVE at 8.3.1 Duration of Border Search at pp. 4-5 ("Special Agents are to complete the search of detained electronic devices . . . in a reasonable time given the facts and circumstances of the particular search."). Furthermore, the U.S. Department of Homeland Security recently completed a review of the legality of suspicionless border searches of digital devices, concluding "that CBP's and ICE's current border search policies comply with the Fourth Amendment." TAMARA KESSLER, OFFICE FOR CIVIL RIGHTS AND CIVIL LIBERTIES, U.S. DEPARTMENT OF HOMELAND SECURITY, CIVIL RIGHT/CIVIL LIBERTIES IMPACT ASSESSMENT: BORDER SEARCHES OF ELECTRONIC DEVICES 2 (2013), [hereinafter 2013 IMPACT ASSESSMENT] *available at* http://www.dhs.gov/sites/default/files/publications/crcl-border-search-impact-assessment_01-29-13_1.pdf.

[15] *See Baseless Searches Of Laptops And Cell Phones Pose Privacy Threats To Travelers*, AMERICAN CIVIL LIBERTIES UNION (January 14, 2010), http://www.aclu.org/national-security/baseless-searches-laptops-and-cell-phones-pose-privacy-threats-travelers. *See also* Stellin, *supra* note 8; Greenwald, *supra* note 9.

[16] *See* U.S. v. Arnold, 533 F.3d 1003 (9th Cir. 2008); U.S. v. Bunty, 617 F. Supp. 2d 359 (E.D. Pa. 2008); U.S. v. Hilliard, 289 F. App'x. 239 (9th Cir. 2008); U.S. v. Romm, 455 F.3d 990 (9th Cir. 2006); People v. Endacott, 79 Cal. Rptr. 3d 907 (Cal. Ct. App. 2008).

[17] For example, in *U.S. v. Arnold*, for purposes of discerning whether a hightened standard of suspicion was necessary to conduct a border search of one's laptop or other digital device, the court there rejected both the argument that one's laptop could be analogized to one's home and the determination as crucial evidence that a laptop could hold an amount of information vastly greater than any typical briefcase or physical container with which one might cross the border. *Arnold*, 533 F.3d at 1009. Furthermore, in his article *Run for the Border: Laptop Searches and the Fourth Amendment*, Nathan Alexander Sales also pinpoints the uniquely private or personal nature of material kept on the laptop and the fact that customs officials might copy and retain data from a person's laptop as additional concerns. Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1110 (2009).

[18] Laptops, for instance, provide access to digital realms removed in space and time from our temporal world, whether in document files or within the internet.

search of one's laptop is certainly taking place at the border, it is also taking place at a digitized location removed from the border, where one's reasonable expectation of privacy may not ultimately reach.[19]

To best understand how the border search doctrine might operate amidst a digital environment (and thereby, what appropriate level of suspicion is needed to lawfully effectuate such a search), this note will train its sights on how the border search doctrine would apply to searches of a particular kind of digital activity: international emails. In doing so, this note will utilize the principles derived therefrom to assess the particular applicability of the border search doctrine to searches of digital devices at our nation's borders, while also identifying the prolonged detention of such digital devices in border searches as both a symptom of the unique digital nature of such devices and one whose corresponding treatment ought to be a "reasonable suspicion" standard for conducting all such searches of laptops and other digital devices at the border.

Towards laying the foundation of this analysis, Part II will address the Fourth Amendment and its applicability to domestic emails, both with regards to the information on the face of the email (including the address and subject of the email) and the content of the email. In addition, Part II will introduce those statutes that have been enacted by Congress towards articulating the standards by which law enforcement may conduct surveillance and intercept both domestic and foreign/international email communications. Part III will turn to the border search doctrine itself and, amidst its seeming applicability to international emails, isolate the reasons behind its practical inapplicability not only by identifying those governmental regulations which all-but-prohibit such searches but also by delving into the constitutional principles that undergird those regulations. Finally, in light of the reasons highlighted in Part III, Part IV will focus upon warrantless, suspicionless searches of laptops and other digital devices at our nation's borders, arguing that the current controversy over prolonged detention of digitial devices in border searches stems from a more fundamental failure to acknowledge the unique spatio-temporal dimensions of digital devices.

I. FOURTH AMENDMENT APPLICATION TO DOMESTIC EMAILS

The Fourth Amendment to the United States Constitution states in relevant part, "[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."[20] With regards to the specific issue of electronic surveillance in a domestic context, the Supreme Court originally held that such surveillance did not constitute a search within the meaning of the Fourth Amendment unless a physical trespass had occurred.[21] However, the Court in *U.S. v. Katz* altered that position, stating that "the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements overheard without any 'technical trespass under property law.'"[22] Indeed, the Court went so far as to clarify that the Fourth Amendment protects people and not places.[23] And yet, as Justice Harlan noted in

---

[19] Regarding the "reasonable expectation of privacy" standard, *see* U.S. v. Katz, 389 U.S. 347, 361 (1967) (J. Harlan, concurring). *See also infra* p. 7 (discussing *U.S. v. Katz*).

[20] U.S. CONST. amend. IV.

[21] Olmstead v. U.S., 277 U.S. 438 (1928).

[22] *Katz*, 389 U.S. at 353 (quoting Silverman v. U.S., 365 U.S. 505, 511 (1961)).

[23] *Id.*

his concurring opinion, "[t]he question . . . is what protection [the Fourth Amendment] affords to those people."[24] To this end, Justice Harlan laid out a two-part requirement for a person to be afforded protection under the Fourth Amendment: she must have both an actual, subjective expectation of privacy as well as an objective, reasonable expectation of privacy.[25]

Hereafter, whether a person was subject to the protections of the Fourth Amendment largely fell upon whether or not she had a "reasonable expectation of privacy," as Justice Harlan delineated in *Katz*.[26] This said, towards determining whether a person has such a reasonable expectation of privacy, the determination is often made by the extent of the governmental intrusion into a person's life. In short, not all intrusions are significant enough to trigger the citizen's reasonable expectation of privacy and afford her protection under the Fourth Amendment. Specifically regarding the governmental act of surveillance, the Court soon drew a bright line in this interplay between a person's reasonable expectation of privacy and the extent of the government's intrusion. In *Smith v. Maryland*,[27] the Court held that a pen register which merely recorded the telephone numbers a person dialed did not abridge that person's reasonable expectation of privacy because the pen register did not access the contents of the telephone calls.[28] The Court reasoned that the telephone numbers dialed were necessarily conveyed to the telephone company for the effect of completing the call and thereby were not within the ambit or control of the person who dialed them such that the person had a reasonable expectation of privacy regarding them.[29]

This distinction—between the information that delineates the source or destination of the message and the content of the message itself—highlights not just the extent to which information is publicly or privately conveyed by a person, nor how far the government can go before a person's reasonable expectations of privacy would be considered overrun. Rather, it re-emphasizes the Fourth Amendment's focus, as explicitly noted in *Katz*, upon the protection it affords to *people*,[30] specifically through the protection afforded to the content of the messages those people have uttered. Certainly, if the petitioner in *Maryland* had spoken his threats on a city street for others to hear, he would not be afforded the protection of the Fourth Amendment because of the public venue for that communication and a consequent lack of any reasonable expectation of privacy that would flow therefrom. However, it is vital to acknowledge not only that the communcation that took place in *Maryland* was via the particular medium of the telephone, but that the electronic configuration of the telephonic communication established a particular environment or "world" that suggested the protected, Fourth Amendment nature of the communication's contents in the first place. In short, *Maryland* (and *Katz* before it) emphasize, albeit indirectly, that the spatio-temporal context of a communication (including the means by which a communication is effected) is a vital component in understanding the extent to which Fourth Amendment protections apply in any given situation.

This contextual reality will take on critical importance when turning to the issue of border searches of both international email communications as well as digital devices, largely because their attendant digital environments are distinct in nature from any kind of telephonic

---

[24] *Id.* at 361 (J. Harlan, concurring).
[25] *Id.*
[26] *Id.*
[27] Smith v. Maryland, 442 U.S. 735 (1979).
[28] *Id.* at 741.
[29] *Id.* at 743.
[30] *Katz*, 389 U.S. at 353.

communication, demanding a particular Fourth Amendment treatment as a consequence. But for now, it remains significant that the "pen register" rule as delineated in *Maryland* finds its internet counterpart without much ado when addressing the applicability of the Fourth Amendment to surveillance of domestic emails. While the Supreme Court has not directly addressed the applicability of the "pen register" rule to email communications, the Ninth Circuit drew several noteworthy parallels between telephonic and email communications towards extending the "pen register" rule to the latter.[31] As telephone users have no reasonable expectation of privacy regarding the telephone numbers they dial because they rely upon the telephone company to complete their communications, so email users "have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."[32] The court also noted that in both instances the content of the communication can only be gleaned through indirect means (such as law enforcement analysis based upon the telephone numbers dialed or email addresses typed in) and are otherwise inaccessible.[33] Finally, the court also extended the "pen register" analogy beyond telephonic and email communications to include regular mail as well, noting how surveillance of the contents of mail packages is afforded Fourth Amendment protection, while the addresses marked on the outside of the packages are not.[34]

Thus, as a general rule, it seems that the content of domestic email communications are afforded Fourth Amendment protection, while any such information conveyed to a third party processor (such as a telephone company, internet provider, or post office) is not. Clearly, such a constitutional analysis finds its sure footing in *Katz*'s "reasonable expectation of privacy" test.[35] It is worth noting, however, the outer boundaries of one's reasonable expectation of privacy with regards to the content of domestic email communications in particular. While one may possess a reasonable expectation of privacy of the contents of an email communication during its transmission, that reasonable expectation of privacy ceases once the email communication has reached its destination, at least with regards to whom the recipient may thereafter share the contents of the email communication.[36] Assuming the recipient does not share the email

---

[31] U.S. v. Forrester, 512 F. 3d 500, 510 (9th Cir. 2007).

[32] *Id.* The Ninth Circuit also noted the active roles of both the telephone company and internet provider in the handling of the information that was ultimately not subject to protection from the Fourth Amendment, suggesting that their expected interaction with the communications, even if minimal, played a role in determining whether Fourth Amendment protection would be afforded to the sender and receiver of the telephonic or email message. ("Like telephone numbers, which provide instructions to the 'switching equipment that processed those numbers,' e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers." *Id.* (quoting *Smith*, 442 U.S. at 742)).

[33] *Id.*

[34] *Id.* at 511.

[35] *Katz*, 389 U.S. at 361.

[36] U.S. v. Lifshitz, 369 F. 3d 173, 190 (2d Cir. 2004); U.S. v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997); U.S. v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996). At least one court has gone further, declaring that email communications are unlike telephonic communications in that, by the mere fact of sending a message over the internet, the party expressly consents to the reproduction of the message, and thereby, possesses no reasonable expectation of privacy regarding the content of the party's email communication. Com v. Proetto, 771 A. 2d 823, 829 (Pa. 2001). With regards to the reasoning behind the cessation of a reasonable expectation of privacy upon the arrrival of one's email communciation, such a justification can be found in the concept of the "false friend," which acknowledges that one possesses no reasonable expectation of privacy with regards to communications that have

communication, however, in a practical if not actual sense one's reasonable expectation of privacy remains intact, once again illustrating that the context surrounding one's email communication plays a vital role in determining the attendant Fourth Amendment protections afforded that communication.

The standards for conducting surveillance of email communications have not been wholly left to the courts, guided as they are by the Constitution. Congress has passed a number of statutes which have gone through various amendments throughout the years, many in response to a heightened need for additional national security safeguards in light of the terrorist attacks on September 11, 2001. First, it is important to note that the case law regarding surveillance of electronic communications, including pen register surveillance, has for all intents and purposes been codified under Title III of the Omnibus Crime Control and Safe Streets Act (Wiretap Act) and its subsequent amendments.[37] Second, with regards to the specific issue of foreign and international communications, through its various amendments the Wiretap Act specifically references and incorporates all relevant provisions within the Foreign Intelligence Surveillance Act (FISA) which addresses the applicable standards for governmental surveillance of both foreign and international communications of an alleged terrorist nature, the latter implicitly.[38]

While FISA's governance of international communications appears, on is face, to implicate similar territorial governance as the border search doctrine, ultimately the statute and doctrine respectively govern the standards for conducting "searches" of distinct areas of alleged criminal activity. As noted previously, the Supreme Court had repudiated the requirement for a physical trespass in matters of governmental surveillance and established a "reasonable expectation of privacy" test.[39] In response, Congress enacted the above-mentioned Wiretap Act which affords citizens upon whom surveillance is enacted all of the typical Fourth Amendment protections, including the need for probable cause to effectuate the ability to procure the requisite warrant.[40] The federal government, however, was not ultimately constrained by these Fourth Amendment requirements honored via the Wiretap Act. Under the auspices of national security, in the late 1960's President Nixon had authorized the CIA and army personnel to conduct warrantless domestic surveillance of Vietnam war protestors, which led to the arrest of several such persons who were accused of plotting to bomb a CIA office in Michigan.[41] When presented with the question of whether the federal government may conduct warrantless surveillance of domestic communications, the Supreme Court held that, while the Wiretap Act did not prevent the President from conducting warrantless surveillance when necessary to protect the nation, this power was constrained within a domestic context by a convergence of protected speech interests under the First Amendment and privacy interests under the Fourth Amendment.[42] Subsequently, after much investigation by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee),[43] Congress enacted FISA as a direct

---

been voluntarily given to another. That other party may then do with them as she may, including supply them to a government officer or agent. *See* Spano v. New York, 360 U.S. 315 (1959).

[37] 18 U.S.C. § 2511 (2012).

[38] 18 U.S.C. § 2511(2)(e-f) (2012).

[39] *See* U.S. v. Katz, 389 U.S. 347 (1967); Berger v. U.S., 388 U.S. 41 (1967).

[40] 18 U.S.C. § 2510-2522 (1968).

[41] *See, e.g.*, Seymour Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES (Dec. 22, 1974).

[42] U.S. v. U.S. District Court for the Eastern District of Michigan, 407 U.S. 297, 303 (1972).

[43] United States Senate, *January 27, 1975: Church Committee Created* http://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm (last visited Feb. 11, 2013).

remedial measure to the government's warrantless surveillance of its citizens.[44] In effect, the act clarified those areas which the government need not procure a warrant to conduct surveillance.[45] Specifically, the 1978 version of FISA permitted warrantless surveillance:

> [T]o acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—(A) the electronic surveillance is solely directed at—(i) the acquisition of the contents of communications . . . used exclusively between or among foreign powers . . . [and] (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.[46]

In this manner, the aim of FISA was to constrain the federal government from conducting warrantless surveillance of its own citizens' communications within the specialized context of terrorist threats to the nation. As a consequence, FISA implicated within its gambit searches of "international" communications that cross the border because of its focus upon foreign elements. That said, while the border search doctrine also seeks to outline the applicable standards for conducting "international" searches whose goal is to "protect the sovereign," the border search doctrine only includes international communications within its gambit as one of many types of border crossings that are subject to routine inspection in the general interest of deterring threats from entering (and thereby, harming) the sovereign.

This fundamental distinction between FISA and the border search doctrine can be best illustrated by the Terrorist Surveillance Program (TSP), which had been instituted by the Bush Administration subsequent to the 2001 amendments to FISA, better known as The Patriot Act.[47] The TSP had effectively eschewed FISA by, in part, not first seeking the requisite approval from the Foreign Intelligence Surveilance Court (FISC) to conduct the surveillance.[48] While the legality of the federal government's bypassing of FISA is dubious at best,[49] the constitutionality of the TSP under the Fourth Amendment remained a separate issue. With this in mind, justification via the border search doctrine was a possibility, specifically with regards to international email communications. Indeed, the Unclassified Report on the President's Surveillance Program (PSP) (previously, the TSP)[50] did establish that at least one government official sought to utilize the border search doctrine, in part, to justify the existence of the PSP.[51]

---

[44] *Times Topics: Foreign Intelligence Surveillance Act (FISA)*, N.Y. TIMES http://topics.nytimes.com/top/reference/timestopics/subjects/f/foreign_intelligence_surveillance_act_fisa/index.html (last visited Feb. 11, 2013).

[45] 50 U.S.C § 1802(a)(1)(A-B) (1978).

[46] *Id.*

[47] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005).

[48] *See* 50 U.S.C § 1802(a)(3) (1978).

[49] *See* Memorandum from Elizabeth B. Bazan & Jennifer K. Elsea, Legislative Attorneys, Cong. Research Serv., Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information 12 (Jan. 5, 2006). *See also* David Cole, *Reviving the Nixon Doctrine: NSA Spying, the Commander-in-Chief, and Executive Power in the War on Terror*, 13 WASH. & LEE J. C.R. & SOC. JUST. 17 (Fall 2006); John Cary Sims, *What NSA is Doing . . . and Why It's Illegal*, 33 HASTINGS CONST. L.Q. 105, 126-27 (2005-06).

[50] OFFICES OF INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE, DEPARTMENT OF JUSTICE, CENTRAL INTELLIGENCE AGENCY, NATIONAL SECURITY AGENCY & OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, No. 2009-0013-AS (July 10, 2009).

[51] *Id.* at 12.

Deputy Assistant Attorney General John Yoo composed a legal memorandum dated November 2, 2001, justifying the legality of the program not upon the strictures laid out in FISA but upon the Fourth Amendment.[52] In doing so, Yoo referenced both the border search search doctrine and the "special needs" doctrine,[53] while NSA Director Hayden also referenced another Fourth Amendment "exception" during a meeting: the need for "hot pursuit" of communications reasonably believed to involve Al-Qaeda.[54] Nevertheless, as FISA was specifically tailored to address the parameters of governmental surveillance in matters related to national security issues, reliance upon the Fourth Amendment and its broad standards for police activity struck many as an end-around FISA (especially as the federal government did not submit applications to the FISC court to conduct such surveillance), whose very existence emanated from an abuse of Presidential powers via warrantless surveillance activities.[55] In this manner, reliance upon the Fourth Amendment and the border search doctrine emanating therefrom in matters relating to national security may ultimately be unwarranted not because the Fourth Amendment does not apply but because the Fourth Amendment is, as Yoo ironically opined in his memorandum, "primarily aimed at curbing law enforcement abuses" and does not tackle the specialized conflict between Fourth Amendment protection of one's privacy and the President's power as Commander-in-Chief to do what is necessary to protect the nation in matters of national security.[56]

II. The Applicability of the Border Search Doctrine to International Emails

A. *The Border Search Doctrine*

Even those international email communications that fall outside of FISA's governance ultimately do not lend themselves to being applicable to the border search doctrine. Rather, email's unique digitized nature functions as the operative force precluding application of the border search doctrine to international emails while also suggesting, in turn, that a hightened "reasonable suspicion" standard for searches of digital devices which possess the capability of transmiting such email communications is in order. But first, towards identifying the unique nature of international email communications and their consequent inapplicability to the border

---

[52] *Id.* at 11. Specifically, Yoo opined in his memorandum that the provisions of FISA did not proscribe the President's powers to conduct surveillance when matters of national security were at stake. However, critics noted that FISA explicitly permits a fifteen day exemption from the requirement to procure a warrant, suggesting that the President's power to conduct surveillance is circumscribed. *Id.* at 12 (citing 50 U.S.C. § 1811 (2012)). Furthermore, while Yoo referenced the Fourth Amendment and not FISA as the ultimate basis for the legality of warrantless searches, Yoo also eschewed the relevance of the Fourth Amendment itself by stating that "electronic surveillance in 'direct support of military operations' did not trigger constitutional rights against illegal searches and seizures, in part because the Fourth Amendment is primarily aimed at curbing law enforcement abuses." *Id.*

[53] *Id.* at 13. Warrantless searches are appropriate "when special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable." *Id.* (quoting Verona School Dist. 47J v. Acton, 515 U.S. 464, 652 (1995) (as quoted in November 2, 2001 Memorandum at 19)).

[54] *Id.* at 15. *See* Warden, MD. Penitentiary v. Hayden, 387 U.S. 294, 298-99 (1967) ("The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others.").

[55] *Id.* at 12. Indeed, references in FISA to the President's powers as Commander-in-Chief suggest that, contrary to Yoo's contention that FISA did not restrict the President's authority to conduct warrantless surveillance in the interest of national security, FISA explicitly had the President's powers in mind.

[56] *Id.* at 12.

search doctrine, an examination of the doctrine itself is in order. In *US v. Ramsey*,[57] customs officials, operating without a warrant, opened for inspection packages that were crossing the United States border from Thailand because they had "reasonable cause to suspect" that the packages contained drugs.[58] These customs officials were authorized to conduct the warrantless search by statute, which states in relevant part: "Any of the officers or persons authorized to board or search vessels may . . . search any trunk or envelope, wherever found, in which he may have a reasonable cause to suspect there is merchandise which was imported contrary to law."[59] Homing in on the "reasonable cause to suspect" standard, the Court found that the customs officials met the statutory standard,[60] while also enunciating that this standard established "a less stringent requirement than that of 'probable cause' imposed by the Fourth Amendment as a requirement for the issuance of warrants."[61]

However, the mere fact that the statutory standard was less than the constitutional standard did not mean that the statute was unconstitutional. Rather, when examining the constitutionality of the statute with regards to the Fourth Amendment, the Court held "[t]hat searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."[62] Towards justifying this position, the Court first noted that the same Congress which had proposed the Bill of Rights (and the Fourth Amendment therein) had, two months prior, enacted a customs statute which "granted customs officials 'full power and authority' to enter and search 'any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed.'"[63] Thus, the power to search at our nation's borders was a distinct power not subject to any requirements or limitations of the subsequently amended Constitution (most relevantly, the Fourth Amendment).[64]

As noted above, in light of this legislative history, the Court validated the Constitutionaity of the statute in question, but the question remains whether there exists any standard to conduct a warrantless search at our nation's borders. For the Court's language strongly suggests that any search at our nation's borders is per se "reasonable" (and thereby satisfies the Fourth Amendment) based on "the single fact that the person or item in question had entered into our country from the outside."[65] Furthermore, while the statute authorized the border search under a lesser standard,[66] the Court eschewed the need for any level of suspicion to

---

[57] U.S. v. Ramsey, 431 U.S. 606 (1977).

[58] *Id.* at 614-15.

[59] *Id.* at 611 (quoting 19 U.S.C. § 482a (1976)). The particular statute is a recodification of Rev. Stat. § 3061, and is derived from Act of July 18, 1866, § 3, 14 Stat. 178.

[60] *Id.* at 614-15.

[61] *Id.* at 612-13.

[62] *Id.* at 616.

[63] *Id.* (quoting Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29).

[64] Following the passing of the Bill of Rights, the Court had occasion to confirm this line of reasoning in Boyd v. U.S., 116 U.S. 616, 623 (1886): "As this act [regulating the collection of duties] was passed by the same Congress which proposed for adoption the original amendments to the Constitution, it is clear that the members of that body did not regard searches and seizures of this kind as 'unreasonable,' and they are not embraced within the prohibition of the amendment."

[65] *Id.* at 619.

[66] *Id.* at 612. The "reasonable cause to suspect" standard essentially echoes the "reasonable suspicion" standard, which is the lesser standard to "probable case" within Fourth Amendment jurisprudence.

conduct the search at the border, opening the door for any and all searches at our nation's borders regardless of even of a modicum of suspicion.

However, it should be noted that the Court's statement that a border search is per se "reasonable" for having occurred at the nation's borders was specifically made with regards to the Fourth Amendment's "probable cause" requirement.[67] In this manner, and especially in light of the Court's validation of the above-mentioned statute which establishes a "reasonable suspicion" standard, it is possible that the standard to conduct a search at our nation's borders is not wholly absent but simply a lesser one than "probable cause."[68] This does not mean, however, that the constitutional standard to be pinpointed is one of "reasonable suspicion" as established by the above-mentioned statute. Rather, while the Court in *Ramsey* distingishes the Fourth Amendment requirements for conducting a search as wholly distinct from the requirements for conducting such a search at our nation's borders, the Court nevertheless cloaks the validity of a search at our nation's borders without probable cause with a basis in "reasonableness."[69] To this end, one might best elucidate the Court's position regarding the standard for conducting searches at our nation's borders as one that does not require probable cause but must still, nevertheless, be "reasonable" pursuant to the Fourth Amendment's prohibition against "unreasonable searches and seizures."[70]

Indeed, the validity of this analysis can be found in those instances where the Court, amidst a specialized context, has amended its per-se-reasonable border search standard to infuse the greater standard of "reasonable suspicion" for the border search. In *U.S. v. Montoya-Hernandez,*[71] the Court adopted a "reasonable suspicion" standard for conducting the more intrusive body cavity search of a person suspected of smuggling drugs through her alimentary canal.[72] Towards doing so, the Court first noted that "[w]hat is reasonable [with regards to the Fourth Amendment] depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself."[73] In this manner, the Court suggested that the ultimate standard for assessing any search, even those that occur at our nation's borders, is not a per-se-reasonable standard that is both unalterable and operates exclusive to the Fourth Amendment, but a presumption of reasonableness that must ultimately be confirmed by the particular context or circumstances within which the search has taken place. Indeed, the Court in *Montoya-Hernandez* further qualified the kind of searches that fall within the per-se-reasonable border search standard when it held, "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant."[74] By qualifying those border

---

[67] *Id.* at 619 ("There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause.").

[68] Indeed, the Court in U.S. v. Montoya-Hernandez, 473 U.S. 531 (1985) did not state that customs officials may open mail absent any standard to do so. Rather, "first-class mail may be opened without a warrant *on less than probable cause*." *Id.* at 538 (emphasis added). In this manner, the Court did not grant customs officials a blank check to open any and all mail that crossed our nation's borders but simply imposed a lesser standard.

[69] *Id.* at 617 ("This interpretation, that border searches were not subject to the warrant provisions of the Fourth Amendment and were "reasonable" within the meaning of that Amendment, has been faithfully adhered to by this Court."). "[T]he Fourth Amendment does not denounce all searches or seizures, but only such as are unreasonable." Carroll v. United States, 267 U.S. 132, 147 (1925).

[70] U.S. CONST. amend. IV.

[71] U.S. v. Montoya-Hernandez, 473 U.S. 531 (1985).

[72] *Id.* at 541-42.

[73] *Id.* at 537.

[74] *Id.* at 538 (emphasis added).

searches which do not require reasonable suspicion, probable cause, or a warrant as "routine," the Court necessarily left open an entire gambit of governmental activity that might fall outside such a "routine" and be deemed an "unreasonable search" via the Fourth Amendment. Finally, when assessing the "reasonableness" of any particular search, including one that occurs at the border, the Court in *Montoya-Hernandez* also stated, "[t]he permissibility of a particular law enforcement practice is judged by 'balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'"[75] In this manner, the Court essentially established the means by which to achieve an assessment of whether the search was reasonable or not. And while the Court stated, "the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is . . . struck much more favorably to the Government at the border,"[76] it remains relevant that a balance is still struck, with the government not afforded a unilateral right to conduct searches at will merely because such searches occur at the border.

Beyond this qualified nature of the seemingly hard-and-fast, per-se-reasonable border search rule, there are a number of further qualifications to the border search rule, all of which are potentially relevant to an analysis of the applicability of the border search rule to international email communications. First, while the border search doctrine certainly applies in a situation where a search occurs at the actual border, the search might also occur at the functional equivalent of the border and the border search doctrine still apply.[77] Examples of such functional equivalents include "searches at an established station near the border, at a point marking the confluence of two or more roads that extend from the border . . . [or] a search of the passengers and cargo of an airplane arriving at a St. Louis airport after a nonstop flight from Mexico City."[78] The standard for these searches is no different from searches at the actual border, so long as they are not "unreasonably intrusive."[79]

Beyond the functional equivalent border searches, courts have also recognized extended border searches while asserting that the reasonable nature of the extended border search is no longer presumed but must be accompanied by "reasonable suspicion."[80] As the Fifth Circuit noted, "[t]he main difference between the functional equivalent of the border search and an extended border search is that the latter takes place after the first point in time when the entity

---

[75] *Id.* (quoting U.S. v. Villamonte-Marquez, 462 U.S. 579, 588 (1983)).

[76] *Id.* at 540.

[77] Almeida-Sanchez v. U.S., 413 U.S. 266, 272 (1973).

[78] *Id.* at 273.

[79] U.S. v. Guzman-Padilla, 573 F.3d 865, 877 (9th Cir. 2009) (quoting U.S. v. Seljan, 547 F.3d 993, 1002-03 (9th Cir. 2008)).

[80] *Id.* at 877-78. At least one court has suggested that the alternative to "reasonable suspicion" is not limited to "no suspicion" but possibly "mere suspicion" as well. US v. Alfonso, 759 F.2d 728, 734 (9th Cir. 1985). Furthermore, it is crucial to note here that at least one court conducted a qualified interpretation of 19 U.S.C. § 482 (previously identified in U.S. v. Ramsey, 431 U.S. 606 (1977), as the statutory authority warranting a border search under a "reasonable suspicion" standard). In U.S. v. Taghizadeh, 41 F.3d 1263 (9th Cir. 1994), the court identified the appropriate border search statute not as 19 U.S.C. § 482, which applies to searches conducted of items "wherever found," *Taghizadeh*, 41 F.3d at 1265, suggesting that this provision instead applies to extended border searches (discussed in the text above-the-line, immediately following the presence of this footnote). Indeed, this would make sense as 19 U.S.C. § 482, like extended border searches, requires reasonable suspicion. Rather, the court in *Taghizadeh* held that 19 U.S.C. § 1582 is the appropriate border search statute, as it requires no suspicion to be effectuated, stating, "[A]ll persons coming into the United States from foreign countries shall be liable to detention and search by authorized officers or agents of the Government" pursuant to regulations prescribed by the Secretary of the Treasury. 19 U.S.C. § 1582 (2006). Regarding these regulations, *see infra* pp. 21-23.

might have been stopped within the country."[81] Specifically, an extended border search might occur when customs agents realize the significance of suspicious circumstances only after an actual border crossing has occurred or the customs agents have delayed the search as an appropriate tactical maneuver.[82] On the other hand, at least one court has concluded that roving border patrols which conduct searches at least twenty miles from the border fall outside the border search exception and thereby require the requisite probable cause to conduct the search via the Fourth Amendment.[83] In this manner, the removal in time and place of the search are relevant factors towards determining if an extended border search has occurred,[84] as such factors are utilized to ensure that the contents to be searched have not been altered from their crossing of the actual/functional equivalent of the border to the time/place when the extended border search thereafter occurred.[85] Furthermore, the requirement for "reasonable suspicion" emanates from the removed nature of the extended border search from the actual or functional equivalent of the border, and thereby finds its justification in that it "intrude[s] more on an individual's normal expectation of privacy."[86]

As will be discussed shortly, both functional equivalent border searches and extended border searches are relevant as analogous concepts to searches of international email communications, specifically in light of the very digital realm through which these communications traverse. Before perceiving international email communications in this light, however, it is also worth noting that the border search doctrine is not limited to those situations in which a person or effect is entering the United States. Rather, the border search doctrine permits U.S. officials to conduct searches of persons and effects departing the United States without reasonable suspicion, probable cause, or a warrant.[87]

Finally, and of crucial importance with regards to the focus of this note, in 1978 the United States Customs Service of the Department of the Treasury instituted two noteworthy regulations related to the requisite standards to be met to conduct searches of mail at our nation's borders.[88] The original versions of these regulations were promulgated in 1973[89] and asserted that customs officials were authorized to inspect any and all incoming international mail except those that only appeared to contain correspondences,[90] in which case a warrant was necessary.[91] Thereafter, in response to the Supreme Court case of *U.S. v. Ramsey*,[92] these regulations were amended in 1978[93] and remain to this day the relevant authority regarding searches of international mail. As a consequence, these regulations are to be read as an extension of the

---

[81] U.S. v. Niver, 689 F.2d 520, 526 (5th Cir. 1982).
[82] *Alfonso*, 759 F.2d at 734.
[83] *Almeida-Sanchez*, 413 U.S. at 273.
[84] *Alfonso*, 759 F.2d at 734.
[85] Alexander v. U.S., 362 F.2d 379, 382 (9th Cir. 1966).
[86] *Alfonso*, 759 F.2d at 734 (citing U.S. v. Caicedo-Guarnizo, 723 F.2d 1420, 1422-23 (9th Cir. 1984)).
[87] U.S. v. Seljan, 547 F.3d 993, 999 (9th Cir. 2009). *See also* U.S. v. Cardona, 769 F.2d 625, 629 (9th Cir.1985) ("The fact that this case involves an exit search does not alter our analysis . . . [since] the border search exception [also] applies to exit searches.").
[88] Examination of Sealed Letter Class Mail by Customs Officials, 43 Fed. Reg. 14,451 (April 6, 1978) (to be codified at 19 C.F.R. pt. 145).
[89] Mail Importations, 38 Fed. Reg. 13,369-13,370 (May 21, 1973).
[90] *Id.* at 13, 370.
[91] *Id.*
[92] U.S. v. Ramsey, 431 U.S. 606 (1977).
[93] Examination of Sealed Letter Class Mail by Customs Officials, 43 Fed. Reg. 14,451.

principles set forth in *U.S. v. Ramsey*.[94] Like its 1973 counterpart, 19 C.F.R. § 145.2 provides that all mail entering the United States is subject to "[c]ustoms examination, except . . . (3) Letter class mail known or believed to contain only correspondence."[95] This provision also qualifies this power granted to customs officials by stating that it is subject to the provision immediately following it.[96] In that amended provision, customs officals are granted the authority to open letter class mail so long as it "appears to contain matter in addition to, or other than, correspondence, provided they have reasonable cause to suspect the presence of merchandise or contraband."[97] Furthermore, in the absence of a warrant or permission granted by the sender or addressee, "[n]o Customs officer or employee shall open sealed letter class mail which appears to contain only correspondence . . . [nor] read, or authorize or allow any other person to read, any correspondence contained in any letter class mail, whether or not sealed."[98] To summarize, then, according to the above regulations as amended in 1978, letter class mail that appears to contain only correspondence cannot be examined by customs officials, while letter class mail can be examined if it appears that matter is contained in addition to the correspondence and customs officials have reasonable cause to suspect that the matter is merchandise or contraband.[99] Finally, these federal regulations prohibit customs officials from reading any such correspondence that is lawfully opened pursuant to a reasonable cause to suspect matter in addition to any correspondence within the mail.[100]

B. *Principles Behind the Standards for Executing Border Searches of Mail*

With the above federal regulations in mind,[101] it is seemingly clear that the border search doctrine essentially does not apply to international emails. Where the border search doctrine adopts a per-se-reasonable standard for conducting searches that cross our nation's border, eschewing any need for reasonable suspicion, probable cause or a warrant,[102] the regulations essentially prohibit any searches of international mail in the absence of reasonable suspicion that such mail contains matter of a criminal sort in addition to its correspondence.[103] However, it is worth noting that the definitions provided within the Code of Federal Regulations of "letter class mail" and "sealed letter class mail" are specifically limited to physical mail and do not suggest the inclusion of email communications within their gambit.[104] In this manner, these regulations may not indeed apply to international emails, though it would be difficult to imagine what standards would apply as the above-mentioned regulations issue forth from the principles outlined in *U.S. v. Ramsey*.[105] Furthermore, as noted in *US v. Forrester*, "[t]he government's surveillance of e-mail . . . is conceptually indistinguishable from government surveillance of

---

[94] *Ramsey* at 612-13, 616.
[95] 19 C.F.R. § 145.3 (2014).
[96] *Id.*
[97] *Id.* § 145.3.
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] *Id.* §§ 145.2, 145.3.
[102] *See* U.S. v. Ramsey, 431 U.S. 606, 616-19 (1977).
[103] 19 C.F.R. § 145.3.
[104] *Id.* § 145.1.
[105] *See Ramsey*, 431 U.S. at 612-16.

physical mail."[106] As a consequence, the rules relating to letter class mail as enunciated in 19 C.F.R. §§ 145.2 and 145.3 would be deemed most likely applicable to such email communications, despite the latter's literal absence from the regulations' purview, narrowly construed.

Whether the regulations literally apply or not is immaterial, however, for a closer look into the border search doctrine will reveal that warrantless searches of international emails under said doctrine would not apply, suggesting that indeed the just-discussed regulations have it right with regards to international emails in addition to regular mail. First, while the border search doctrine would arguably permit federal officials to search any and all mail that either enters or leaves the nation, these regulations seemingly do the opposite (and despite the fact that the regulations were amended in light of the border search doctrine as enunciated in *Ramsey*): they prohibit searches of any mail with the lone exception in cases where the mail appears to contain matter in addition to correspondence *and* the customs official possesses a reasonable suspicion that the matter is either contraband or merchandise.[107] Set against the backdrop of the border search doctrine, this regulation suggests two principles regarding the search of international mail. First, the information (or correspondence) contained as a part of the thing to be searched is afforded greater protection than any physical or tangible items that are crossing the border. Indeed, 19 C.F.R. § 145.3 essentially affords absolute protection to such information, absent customs officials' procurement of a warrant or consent from either the sender or addressee.[108] As these latter exceptions essentially abide by the edicts of the Fourth Amendment, the border search doctrine does not apply with regards to mail correspondences.

That said, as a second principle, the border search doctrine presumably does apply to mail via the regulation's exception for matter in addition to the correspondence, though the doctrine's applicability is only partial. Specifically, the mail must "appear" to contain matter in addition to correspondence, and the customs official must have a reasonable suspicion that the matter is either contraband or merchandise.[109] In this manner, there are two levels of scrutiny, and both appear to operate within a "reasonable suspicion" standard. First, the fact that the package must "appear" to contain matter in addition to any correspondence suggests customs officials must possess a reasonable suspicion.[110] Then, customs officials also must have a "reasonable suspicion" that the matter is either merchandise or contraband.[111] On the one hand, this dual layer of "reasonable suspicion" both cements the appropriate standard for searches of such matter as "reasonable suspicion" while presumably inching the standard towards "probable cause" via its double layer. Of course, the "probable cause" necessary to fulfill the requirements of the Fourth Amendment cannot be quantified as a double layer of "reasonable suspicion," but the fact remains that (a) the border search rule finds limited application to searches of international mail, and (b) the protection afforded all mail (whether merely correspondence or correspondence with additional matter) is greater than that afforded by in-person entry to, or departure from, the nation.

---

[106] US v. Forrester, 512 F.3d 500, 511 (9th Cir. 2007). ("The privacy interests in [both email and regular mail] communication[s] are identical.").

[107] 19 C.F.R. § 145.3.

[108] *Id.*

[109] *Id.* In the case of email, the additional "matter" might be an attachment to the email. *See infra* p. 28.

[110] *Id.*

[111] *Id.*

However, federal agents' greater authority to conduct searches via the border search doctrine is not wholly absent in border searches of mail via the relevant provisions in the Code of Federal Regulations. Rather, it has gained a foothold by permitting a less-than-probable cause standard for searching mail that appears to contain matter which the customs official has reason to suspect is either merchandise or contraband.[112] Towards appreciating why the principles behind the border search doctrine might intrude upon searches of mail in this manner, it is important first to identify the tangible nature of the thing to be searched as the variable at play in enunciating this less-than-probable cause standard. While "correspondences" (and the corresponding thoughts, ideas, feelings, and personhood attendant to them) are subject to the probable cause requirement, objects of a tangible nature that accompany such correspondences are subject to the lesser standard of "reasonable suspicion" (even if, as already noted, this lesser standard is applied doubly). Two important points can be derived therefrom. First, the regulations implicitly afford great value and protection to the personal privacy and dignity contained within the correspondences by granting it traditional "probable cause" Fourth Amendment protection. Second, while the matter accompanying such correspondences would typically not embody the privacy and dignity of a person (unlike the manner in which words can embody such privacy and dignity), the tangible nature of such "matter" poses a potential danger to the sovereign that is not otherwise protected by the Constitution.[113] As a consequence, it can be presumed that the standard to conduct searches of such matter as "reasonable suspicion" is less for that reason.

As discussed previously in this note, the "reasonable suspicion" standard has been applied in other contexts amidst the border search doctrine.[114] First, however, it is worth recalling that the border search doctrine, sans a "reasonable suspicion" standard, typically applies when a physical crossing of our nation's borders has occurred.[115] In this manner, the Code of Federal Regulations has distinguished searches of such tangible "matter" based upon the mode of transit in crossing our nation's border; in short, the federal government affords more protection to mail (whether or not it contains "matter") when it crosses the border than when a physical, in-person crossing has occurred. Such greater protection is not reserved, however, only for mail when it crosses our nation's borders. For, amidst the border search doctrine, a "reasonable suspicion" standard is also applied (as noted previously) in an "extended border search."[116] The justification behind this increased protection can be found in the fact that the extended border search takes place not at the actual border or the functional equivalent of the border, but already within the nation's borders where typical Fourth Amendment "probable cause" protection would be afforded.[117] In addition, a "reasonable suspicion" standard was also adopted amidst the context of the border search doctrine in situations where the search to be performed was more

---

[112] *Id.*

[113] As one's words would be protected by the First Amendment. *See* U.S. CONST. amend. I.

[114] *See supra* p. 18 and accompanying note 71 (body cavity search); *see also supra* pp. 20-21 and accompanying notes 79-81 (extended border search).

[115] *See* U.S. v. Ramsey, 431 U.S. 606, 616 (1977).

[116] *See supra* p. 20 and accompanying note 79.

[117] U.S. v. Niver, 689 F.2d 520, 526 (5th Cir.1982). For there to be an extended border search, the search must still retain both a qualifiable and quantifiable connection to an actual or functional equivalent border search. As noted previously, the time elapsed from crossing the border and the distance from the actual or functional equivalent border are important factors. *See supra* pp. 20-21 and accompanying notes 83-84. However, the extended border search must still issue forth from a search that could have been conducted at the actual or functional equivalent border if it weren't for exigent circumstances. *See* Alexander v. U.S., 362 F.2d 379, 382 (9th Cir. 1966).

invasive (such as a body cavity search[118]) and thereby infringed to a greater extent upon the privacy concerns of those crossing the border.[119] Finally, it is crucial to emphasize that the above principles as derived from both regulatory and constitutonal authority must coalesce within the Fourth Amendment's prohibition against "unreasonable searches."[120] In short, any and all search practices by the federal government must conform to the standard of being "reasonable."

C. *Applying the Border Search Doctrine to International Emails*

Towards applying the principles drawn from an analysis of both regulatory authority and "border search doctrine" case authority to the question of the applicability of the border search doctrine to international emails, it is first crucial to identify the specific parameters of email as "mail" within the relevant Code of Federal Regulations provisions. The Code of Federal Regulations speaks of both correspondences and matter in addition to such correspondences.[121] On the one hand, one can easily envision the applicability of "correspondences" to email, as email most often involves a sender "mailing" a text message to a particular addressee. Furthermore, as email is executed in a digital format, it cannot possess "matter" as such to accompany such correspondences to the extent that "matter" connotes a physicality. Nevertheless, the email equivalent of "matter" in such circumstances is ultimately not too hard to envision, as it suggests "attachments" a sender can execute along with his/her correspondences. However, with regards to the "reasonable suspicion" standard applicable to customs officials when executing warrantless searches of international email, the matter (no pun intended) becomes less straightforward. First, it remains uncertain whether a goverment official (via the pen register rule[122]) can perceive that an email "appears" to contain matter in addition to its correspondence.[123] Assuming it can, it then becomes easy to apply the regulations to international email, as the requisite "reasonable suspicion" that the matter is "merchandise" might refer to a downloadable software, while the "contraband" might be child pornography or "matter" in violation of IP laws.

Having nestled international email within the regulations in question, it is now appropriate to address the applicability of international email to the border search doctrine amidst the Fourth Amendment requirement that any search must be "reasonable."[124] Towards doing so, one might begin by asking, "Is it reasonable for the government, pursuant to the border search doctrine, to conduct warrantless searches of international email without reasonable suspicion, probable cause or a warrant?" A knee-jerk reaction might answer in the negative, but

---

[118] *Montoya-Hernandez*, 473 U.S. at 541-42.

[119] *Alfonso*, 759 F.2d at 734 (citing U.S. v. Caicedo-Guarnizo, 723 F.2d 1420, 1422-23 (9th Cir. 1984)).

[120] U.S. CONST. amend. IV.

[121] 19 C.F.R. § 145.3 (1978).

[122] Smith v. Maryland, 442 U.S. 735 (1979).

[123] According to the website *Surveillance Self-Defense*: "By serving a pen/trap order on your ISP or email provider, the police can get . . . [a]ll email header information other than the subject line, including the size of each email that is sent or received . . . [as well as] [t]he communications ports and protocols used, which can be used to determine what types of communications you are sending using what types of applications." *Surveillance Self-Defense: "Pen Registers" and "Trap and Trace Devices,"* ELECTRONIC FRONTIER FOUND., https://ssd.eff.org/wire/govt/pen-registers (last visited February 11, 2013). Because the government can discern the size of an email, it is reasonable to suppose that the government can discern thereof whether there is "matter in addition to" the email as a correspondence. 19 C.F.R. § 145.3.

[124] U.S. CONST. amend. IV.

via a utilization of the principles derived from the previous section's discussion, a more grounded answer is within arm's reach. First, the prohibition against searches of correspondences is both "reasonable" insofar as it protects the privacy interests of the individual and acknowledges that the government's interest in protecting the sovereign from an individual's words is not one the border search doctrine had in mind within its goal to protect the sovereign.[125] Indeed, as lesser standards to conduct warrantless searches are imposed on government officials with regards to physical, in-person border crossings and mail crossings that involve matter in addition to any correspondence, it is clear that the sovereign primarily seeks to protect itself from tangible, physical threats. In this manner, one can read the double layer of "reasonable suspicion" protection for mail that contains matter in addition to correspondence as emphasizing the individual's privacy interests against the sovereign's right to protect itself from tangible threats via a balancing of Fourth Amendment interests.[126] Furthermore, while a greater standard is imposed for searches that are more intrusive (such as the previously noted body cavity search[127]), one could use this principle to justify the greater protection afforded mail and its correspondences contained therein, as any such searches would be deemed necessarily "intruding" upon the privacy interests of individuals.[128] Finally, as the extent of the applicability of the border search doctrine corresponds to its qualifiable and quantifiable connection to said border, the dubious existence of an identifiable border within the context of international email further suggests the inapplicability of the border search doctrine to international emails. On the one hand, it is clear that, ex post facto, a government official can determine if an email was sent across the nation's borders. However, the very idea of enforcing the nation's digital borders via the border search doctrine is muddied by two realities: (1) the circuitous route of all emails, including domestic emails, renders them "international";[129] and (2) the likelihood that a search of an international email could be conducted at the actual or functional equivalent border is highly unlikely given the relatively borderless nature of the internet.[130] Regarding the former, all emails, in actuality, are not sent from (for example) my computer in Naples, Florida to an addressee in (for example) Chicago, Illinois.[131] Rather, emails are routed through servers that may be domestic or international, while emails also often enter a cyber-realm where no one can actually tell where the email is at any given time.[132] Even if lawmakers would eschew such a literal analysis of the path of an email for the more practical Naples-to-Chicago reality, the fact remains

---

[125] U.S. v. Montoya-Hernandez, 473 U.S. 531, 538 (1985) (quoting U.S. v. Villamonte-Marquez, 462 U.S. 579, 588 (1983)) ("The permissibility of a particular law enforcement practice is judged by 'balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'").

[126] *Id.*

[127] *See supra* p. 18.

[128] The stricter standard imposed for the intrusive body cavity search in *US v. Montoya-Hernandez* implicitly did define such an intrusion as physical in nature. Nevertheless, the implicit acknowledgement via 19 C.F.R. § 152.3 that searches of correspondence would likewise be intrusive remains relevant and applicable to this constitutional analysis. Indeed, the Court's determination in *Cotterman (2013)* (to be addressed at the conclusion of this note, *see infra* note 166) that forensic analysis of digital devices in border searches requires reasonable suspicion because of its highly intrusive nature supports this reasoning. *See* U.S. v. Cotterman, 709 F.3d 952, 964-65 (9th Cir. 2013).

[129] *Chapter 7. How Email Really Works*, KAVI HELP CTR., (Jan. 21, 2014), https://groups.wi-fi.org/khelp/kmlm/user_help/html/how_email_works.html.

[130] *See, e.g.*, *The Borderless Internet and Jurisdictional Disputes: A Growing Problem*, TECHDIRT, http://www.techdirt.com/articles/20090804/0045095760.shtml (last visited February 10, 2013).

[131] *Chapter 7. How Email Really Works*, KAVI HELP CTR., (Jan. 21, 2014), https://groups.wi-fi.org/khelp/kmlm/user_help/html/how_email_works.html.

[132] *Id.*

(as stated in the latter point) that the border search doctrine's actual and functional equivalent border possesses no congizable meaning in a cyber-digital context.[133] One would have to either re-define the meaning of a "border" for the border search doctrine to apply to international emails or suggest that any warrantless search of international email executed via the border search doctrine operate from the "extended border search" rule. This would account for the reality that any such search cannot practically occur at the border (given the very problem of establishing a cognizable border in an internet context) while the search would then occur amidst a qualifiable and quantifiable relation to the border.

For example, if someone in Germany sends an email with an attachment of child pornography to someone in the United States, the federal government might search the email soon after its arrival, so long as the time elapsed might be deemed reasonable within the Fourth Amendment.[134] To conduct such an extended border search, of course, the government must have "reasonable suspicion,"[135] but then such a requirment of reasonable suspicion merely corresponds with the regulatory requirement under 19 C.F.R. § 152.3 that searches of matter accompanying correspondences be conducted only after the government has reasonable suspicion that the mail contains contraband or merchandise.[136] The "extended border search" rule applies the "reasonable suspicion" standard to the warrantless search as a whole while the regulatory provision applies the same standard to only one portion of the thing to be searched (the "matter" within the mail), but one must keep in mind that the extended border search standard applies to tangible, in-person border crossings while the regulatory standard within 19 C.F.R. § 152.3 applies to that portion of the mail that crossed the border that is likewise tangible: the mail's "matter" accompanying the correspondence. In this manner, if the border search doctrine were to be applied to international emails, given the particular digital context within which the mail was transmitted and the tangible nature of the items to be searched, a "reasonable suspicion" standard would be appropriate for the warrantless search of international emails within the regulatory context supplied by 19 C.F.R. § 152.3, which limits such searches to the matter that accompanies any such correspondences.

III. Reasonable Suspicion to Conduct Warrantless Searches of Digital Devices at Our Nation's Borders

Indeed, it is my contention that this "reasonable suspicion" standard, insofar as it is applicable to the "matter" within international emails, should be applicable to any such searches of those tangible objects, such as laptops and smart phones, at our nation's actual or functional equivalent borders. Nevertheless, as articulated in the Introduction to this note, the federal

---

[133] One might suggest that the "functional equivalent" of a border search in the digital context occurs upon the ex post facto determination that an email has been sent across the nation's borders, but then such a interpretation would necessarily butt up against the reality that the email is now either nestled well within or well beyond the nation's borders, seemingly affording the email to be searched in the former instance all the protections of the Fourth Amendment's "probable cause" requirement, while in the latter the email is either subject to governance under FISA or outright beyond the United States' jurisdiction.

[134] U.S. Const. amend IV.

[135] U.S. v. Guzman-Padilla, 573 F.3d 865, 877-78 (9th Cir. 2009) (quoting U.S. v. Seljan, 547 F.3d 993, 1002-03 (9th Cir. 2008)).

[136] 19 C.F.R. § 152.3 (1978).

government has asserted that searches of such digital devices require no reasonable suspicion,[137] a position federal courts have consistently supported.[138] For example, the court in *U.S. v. Arnold*[139] held that no such reasonable suspicion standard was applicable to border searches of laptops and other such digital devices because that particular kind of search did not fall within the narrow exceptions outlined previously by the Supreme Court.[140] Pursuant to the Supreme Court's holding in *U.S. v. Flores-Montano*,[141] the *Arnold* court categorized two kinds of intrusive searches that would necessitate the application of the reasonable suspicion standard: searches of a person and searches of property.[142] Regarding the latter, the Supreme Court limited any possible application of the reasonable suspicion standard for searches of property to ones that are "so destructive" without expounding on the parameters that might meet such a standard.[143] Meanwhile, regarding the former, the Supreme Court emphasized the "dignity and privacy interests of the person being searched" as the touchstone from which to assess whether or not to apply a "reasonable suspicion" standard,[144] though the Supreme Court ultimately chose to "leave open the question 'whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out.'"[145]

When applying the Supreme Court's standard for reasonable suspicion, the *Arnold* court emphasized that searches of property (whether of the vehicle in *Flores-Montano*[146] or laptop computers) do not implicate the same type of privacy concerns as searches of people.[147] In addition, the court held that, unlike searches of a person, an intrusiveness analysis is essentially inapplicable in the context of property searches, where the goal might otherwise be to determine

---

[137] 2009 CBP DIRECTIVE, *supra* note 11, at 3 ("5.1.2 In the course of a border search, with or without individualized suspicion, an Officer may examine electronic devices and may review and analyze the information at the border . . . ."); 2009 ICE DIRECTIVE, *supra* note 12, at 2 ("6.1 ICE special agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion, consistent with the guidelines and applicable laws set forth therein."); 2013 IMPACT ASSESSMENT, *supra* note 13, at 2. Regarding the 2009 CBP DIRECTIVE, the dissenting voice in *U.S. v. Cotterman* stated, "[the federal government] could . . . translate any documents in a foreign language, ensure that [no] seemingly innocuous pictures are actually encrypted messages, verify the licenses on any music or movies on the computer, review financial logs for evidence of insider trading, *read email correspondence* to ensure that there is no communication with known criminals—the list of possible "concerns" is endless . . . ." U.S. v. Cotterman, 637 F.3d 1068, 1086 n.5 (9th Cir. 2011) (Fletcher, J., dissenting) (emphasis added).

[138] *See* U.S. v. Bunty, 617 F. Supp. 2d 359 (E.D. Pa. 2008); U.S. v. Hilliard, 289 F. App'x. 239 (9th Cir. 2008); U.S. v. Romm, 455 F.3d 990 (9th Cir. 2006); People v. Endacott, 79 Cal. Rptr. 3d 907 (Cal. Ct. App. 2008). Some circuit courts of appeals have avoided the question of whether reasonable suspicion is necessary by finding reasonable suspicion anyway within the particular facts before them. *See* U.S. v. Bunty, 617 F. Supp. 2d 359 (E.D. Pa. 2008); U.S. v. Irving, 452 F.3d 110 (2d Cir. 2006); U.S. v. Furukawa, 2006 WL 3330726 (D. Minn. 2006). As noted previously, *Cotterman (2013)* represents the only decision to impose a "reasonable suspicion" standard on searches of digital devices at the border, limited to the particular situation where a forensic analysis of the digital device is conducted. *See* U.S. v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013). *See also supra* note 5.

[139] U.S. v. Arnold, 533 F.3d 1003 (9th Cir. 2008).

[140] *Id.* at 1007.

[141] U.S. v. Flores-Montano, 541 U.S. 149 (2004).

[142] *Id.* at 152.

[143] *Id.* at 155.

[144] *Id.* at 152.

[145] *Id.* at 155, note 2 (quoting U.S. v. Ramsey, 431 U.S. 606, 618, n. 13 (1977)).

[146] *Id.* at 150.

[147] *Arnold*, 533 F.3d at 1008 (citing Flores-Montano, 541 U.S. at 152).

whether such a search was routine or nonroutine.[148] Finally, as referenced previously, the *Arnold* court also dismissed two efforts by the petitioners to analogize searches of laptops at the border to other kinds of searches that would require a hightened standard of scrutiny.[149] First, the court rejected the analogy of a "home" to one's laptop,[150] where the vast array of personal information contained therein functions as the digital counterpart to the tangible personal items that make up one's home. Second, the *Arnold* court rejected the argument that a search could be highly invasive based upon the size or capacity of the storage container to be searched.[151]

Though a discussion could be had challenging the reasoning behind the *Arnold* court's holding on the above-mentioned issues, the emphasis here will be on establishing that (1) not all property to be searched is equal, and (2) as emails function as a representation of the type of digitized information to be searched within a laptop or other digital device, the rules as applicable to searches of international email are likewise appropriate to such digital devices as well, albeit altered slightly to account for the search of tangible property (i.e. the laptop itself) at an actual or functional equivalent border crossing.

First, while is is true that the Supreme Court has suggested that a reasonable suspicion standard might only be appropriate for searches of property if such searches are "so destructive," one must keep in mind that the Court's assertion was made amidst the context of assessing whether such a "destructive" act was made pursuant to the gas tank on a car.[152] Such an item is strictly "property" in the classical sense, in that it does not (or only does so to a minimal extent) assume or take upon itself the personhood of its owner. In short, if the ultimate goal is to assess the reasonableness of a search pursuant to the Fourth Amendment, it would be inapproprate to apply a set standard for all property (e.g. "the risk of physical destruction must be great to warrant reasonable suspicion to conduct such a search") when not all pieces of personal property possess the same kind of relation to the person who owns them.[153] With this in mind, clearly such a piece of property as a laptop or smart phone possesses a greater measure of personhood than a gas tank, if anything for the digital device's ability to embody and transmit the person's thoughts and expressions.[154] On the other hand, such digital devices most probably contain "matter" in addition to any strict expressions or embodiments of the person who owns it. As an

---

[148] *Id.* In the Ninth Circuit's decision in *Cotterman (2013)*, the court interjected an intrusiveness analysis concerning the property of a laptop seemingly at odds with its holding in *Arnold*. *See* U.S. v. Cotterman, 709 F.3d 952, 964-66 (9th Cir. 2013).

[149] *See supra* note 16.

[150] *Id.* at 1009.

[151] *Id.*

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

[153] U.S. v. Montoya-Hernandez, 473 U.S. 531, 537 (1985) (As noted in *Montoya-Hernandez*, what is reasonable pursuant to the Fourth Amendment depends upon surrounding circumstances).

[154] One might envision a purse or briefcase as a "personal" container better suited to analogize with a laptop, while also noting that searches of such "personal containers" as a purse or briefcase have not been afforded greater protection. *See* U.S. v. Soto-Teran, 44 F. Supp. 2d 185, 190 (E.D.N.Y. 1996), *aff'd*, 159 F.3d 1349 (2d Cir. 1998) (quoting U.S. v. Turner, 639 F. Supp. 982, 986 (E.D.N.Y.1986) (quoting U.S. v. Grotke, 702 F.2d 49, 51–52 (2d Cir. 1983))) ("A routine search may include 'a person's luggage, personal belongings, outer clothing, wallet, purse, and even one's shoes.'"). However, as will be discussed shortly, it is both the personal nature of the laptop or other digital device when coupled with its unique connection to a removed, digital realm which warrants increased protection. *See infra* pp. 36-38. Furthermore, in *Cotterman (2013)*, the Ninth Circuit has clarified its previous position in *Arnold* regarding searches of digital devices to permit an intrusiveness analysis that acknowledges the invasion into one's privacy that a forensic analysis of a laptop can occasion. *See* U.S. v. Cotterman, 709 F.3d 952, 964-66 (9th Cir. 2013). *See also infra* p. 40.

extreme example, such digital devices could contain contraband in the form of child pornography. In this manner, the property item to be searched (the laptop or other digital device) possesses a dual life as both a container of "matter" and an extension or embodiment of the person who owns it. The question then becomes, how ought the laptop or digital device be treated for purposes of a warrantless search at the actual or functional equivalent of our nation's borders?

On the one hand, a clear distinction can be made between the border searches of such "matter" via mail (whether regular mail or email) and at the actual or functional equivalent of the border. While the border search of matter accompanying correspondences transmitted as mail is subject to a reasonable suspicion standard, no such reasonable suspicion is required at the actual or functional equivalent of the border. In this manner, the laptop's capacity as a container to hold "matter" suggests that border officials do not need any suspicion to conduct a search of a laptop based upon this particular property quality. On the other hand, the laptop or digital device also possesses the capacity, like regular mail or email, to both hold or trasmit the correspondences or expressions of its owners. And by embodying, both literally and figuratively, the qualities of such mail, the laptop also thereby incorporates the very principles that undergird the heightened protection afforded such correspondences/expressions as provided in the Code of Federal Regulations.[155] Once again, the relevant provisions prohibit any searches of the correspondences of such mail absent probable cause, a warrant, or consent,[156] even though the search to be effectuated takes place at our nation's borders. This premium placed upon the privacy, via their mail correspondences, of those crossing the border would certainly have to be amended in the instance of a physical border crossing, especially in light of the sovereign's desire to protect itself from tangible threats.[157] Thus, the need for probable cause to conduct a search of mail correspondences would appropriately translate to a need for reasonable suspicion to inspect such correspondences (as embodied in the digital device) in an in-person border crossing.

While it seems that an impasse has been struck with regards to the appropriate standard to be conducted concerning laptops and other digital devices at our nation's borders, it must be noted that in an in-person border crossing a "reasonable suspicion" standard does not apply with regards to the search of such correspondences or expressions that might assume a tangible form on paper, in notebooks, etc.[158] In this manner, the argument for greater protections for the searches of laptops appears to be an argument not for added safeguards for the actual correspondences or expressions, but an argument concerning one's "reasonable expectation of privacy"[159] regarding those correspondences amidst their digital environment. In short, while one "reasonably expects" customs officials, during an in-person tangible search, to conduct an in-person tangible search of one's person and effects, the digital nature of a laptop's contents strikes the traveler as removed from the scope and ambit of the search.[160] For instance, while it would

---

[155] 19 C.F.R. §§ 145.2, 145.3 (1978).

[156] *Id.*

[157] As embodied by its lessening standard for warrantless searches for in-person border crossings as opposed to mail crossings.

[158] *See* U.S. v. Taghizadeh, 41 F.3d 1263, 1266 (9th Cir. 1994); U.S. v. Glasser, 750 F.2d 1197, 1200–05 (3d Cir. 1984), cert. denied, 471 U.S. 1018, (1985); U.S. v. Pringle, 576 F.2d 1114, 1116 (5th Cir. 1978); *Soto-Teran*, 44 F. Supp. 2d at 190.

[159] U.S. v. Katz, 389 U.S. 347, 361 (1967) (J. Harlan, concurring).

[160] *See, e.g.*, Lauren Guicheteau, *No Civil Rights Violations for Suspicionless Border Searches of Electronic Devices*, LAW, TECHNOLOGY & ARTS BLOG, 4 (February 20, 2013), http://wjlta.wordpress.com/category/university-of-washington-school-of-law/ ("[M]any people see electronic

certainly be appropriate for customs officials to conduct a search of the physical inner workings of a laptop (to ensure that it does not conceal a bomb, for instance), a search of the digital inner workings of the laptop strikes one as less appropriate for the very fact that the digital realm being searched is only incidentally connected to the physical place where the search is being conducted. In this manner, the laptop or digital device operates as not merely a container which stores "files" but more significantly as a key that provides access to a digital realm that is removed from any physical spatio-temporal location (and is most widely represented by the internet), most notably the border at issue. As a consequence, towards evaluating the reasonableness of such a search of a digital device at our nation's borders, this context of a digital device being not just a container (as a briefcase is a container) but a means to access a digital realm that is removed both in time and space from the physical locale of the search is vital. Indeed, given the removed nature of the digital realm which the digital device provides access to, it would be appropriate to label the search of such a device at the actual or functional equivalent border as an "extended border search" which thereby necessitates reasonable suspicion.

This said, it is understandable that courts have chosen to treat laptops and other digital devices as merely more modern counterparts to such traditional containers as briefcases which, like a laptop, can contain one's files. After all, reliance upon the past is a trademark of legal thought embodied by what is a foundation of the law: reliance upon precedent to determine what is the law (i.e. "legalism"). However, towards truly satisfying the Fourth Amendment requirement that, for a seach to be reasonable, it must "[depend] upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself,"[161] an acknowledgement that a laptop or digital device is much more than a container is crucial. For it is the digital device's ability as a key to unlock and gain access to the digital world which necessarily removes the search of such a laptop or digital device from the actual or functional equivalent border and re-positions the search to a spatio-temporal position beyond said border. This does not mean, however, that laptops and other such digital devices at our nation's borders ought to then be treated as if already fully within our nation's borders and afforded, thereby, all the Fourth Amendment protections attendant thereto. For the other reality at play is that the search is, in another very tangible sense, taking place at the actual or functional equivalent border. Thus, by taking into consideration the fact that the search takes place both at our nation's borders and (digitally speaking) above-and-beyond it, a "reasonable suspicion" standard honors both realities and ultimately validates the Fourth Amendment's prononcement against unreasonable searches and seizures.[162]

CONCLUSION

As noted at the inception of this note, this call for a "reasonable suspicion" standard for conducting searches of digital devices at the border may strike some as coming a day—if not a year or two—late.[163] After all, prior to the Ninth Circuit's recent decision in *U.S. v. Cotterman (2013)* which required reasonable suspicion to conduct a forensic analysis of a digital device at

---

devises as unique in their vast storage capacity of personal information and the ability to track its user's preferences and habits, which should distinguish them from other types of baggage.").

[161] U.S. v. Montoya-Hernandez, 473 U.S. 531, 537 (1985).

[162] U.S. CONST. amend IV.

[163] *See supra* p. 4.

the border,[164] the controversy over suspicionless searches of digital devices at the actual or functional equivalent border had been all-but-settled[165] and given way to a new controversy: the prolonged detention of such digital devices in an actual or functional equivalent border search. However, one must keep in mind that the source of this current controversy over prolonged detention of digitial devices in border searches is not necessarily a blatant abuse of governmental power. Rather, the complex, technological nature of the digital device demands that, if a search is going to be conducted that adequately serves to protect the sovereign, measures must be taken to effectuate that search which may involve the enlistment of experts and protocols that take time and necessitate a removal from the actual or functional equivalent border.[166] In addressing these realities, the Ninth Circuit in *Cotterman (2013)* attempted to distinguish the prolonged detention of a digital device in a border search from the act of conducting a forensic analysis of the digital device, asserting that only the latter requires reasonable suspicion.[167] The court held, "[i]t is the comprehensive and intrusive nature of a forensic examination—not the location [or duration] of the examination—that is the key factor triggering the requirement of reasonable suspicion here."[168] Accordingly, the court aligned such a forensic analysis with the body cavity search in *U.S v. Montoya-Hernandez*,[169] "implicating substantial personal privacy interests."[170] As such, the *Cotterman (2013)* court's argument implicated a distinct concern from the argument in this note, whose focus is upon the unique spatio-temporal nature of digital devices.[171] Further, in dismissing the factors of time and location in its analysis, the court failed to appreciate the unique spatio-temporal interplay at work in all border searches of digital devices. In short, the prolonged detention of digital devices in border searches issues forth from those devices' unique digitized nature which, as stated previously, is necessarily removed in a spatio-temporal sense from the actual or functional equivalent border where such searches take place.

---

[164] U.S. v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013).

[165] Once again, the Supreme Court has not officially spoken on the issue of warrantless searches of digital devices.

[166] *See* 2009 CBP DIRECTIVE, *supra* note 11, at 5 ("5.3.2.1 The use of other federal analytical resources . . . such as translation, decryption, and subject matter expertise, may be need to assist CBP in reviewing the information contained in electronic devices or to determine the meaning, context, or value of the information contained in electronic devices"); *See also* 2009 ICE DIRECTIVE, *supra* note 12, at 5 ("8.4(1)(a) During a border search, Special Agents may encounter information in electronic devices that present tecnical difficulties, is in a foreign language, and/or encrypted. To assist ICE in conducting a border search or in determining the meaning of such information, Special Agents may demand translation, decryption, and/or technical assistance from other Federal agencies or non-Federal entities."). With regards to both the 2009 CBP DIRECTIVE and the 2009 ICE DIRECTIVE, if Special Agents encounter information in a search of a digital device that does not present technical difficulties, is not in a foreign language, and not encrypted but still necessitates the assistance of subject matter experts to determine the nature of the material under scrutiny, such Special Agents can do so but only if they have a reasonable suspicion of a violation of laws. 2009 CBP DIRECTIVE at 5; 2009 ICE DIRECTIVE at 6. This self-imposed restriction suggests that the federal government's motives for detaining laptops is not guided by an agenda beyond the practical necessities in doing so.

[167] *Cotterman*, 709 F.3d at 957.

[168] *Id.*

[169] U.S. v. Montoya-Hernandez, 473 U.S. 531, 541-42 (1985).

[170] *Cotterman*, 709 F.3d at 964.

[171] For example, when the *Cotterman (2013)* court asserted, "Moving the laptop to a specialized lab at a distant location might highlight that the search undertaken there was an extensive one, but it is not the dispositive factor here," *Id.* at *6, the court's focus upon the "extensive" nature of the search illustrated that the factors of time and distance were only viewed by the court through the "substantial personal privacy interests" at stake, *Id.* at *7, and not, as in this note, with regards to the unique and fundamental spatio-temporal position at play between the border and digital devices.

In this manner, the controversy over prolonged detentions of digital devices in border searches evinces a "reasonable suspicion" standard not only in those specific instances where the digital device is detained for a prolonged period of time (or when a forensic analysis of the digital device is conducted[172]), but in all border searches of digital devices because the digital device itself is already "extended" or removed in a very real sense from the actual or functional equivalent border. One might question the impact of implementing a "reasonable suspicion" standard in all border searches of digital devices upon those searches that do result in a prolonged detention. Would the decision to "extend" the border search in time and/or location necessitate an additional layer of scrutiny, not unlike the double layer of "reasonable suspicion" implicit in 19 C.F.R. § 152.3?[173] While on the surface such a spatio-temporal removal of the border search might appear to implicate a second "extended border search," one must keep in mind that the search's removal via a prolonged detention issues forth from the very source that occasioned the reasonable suspicion standard at the actual or functional equivalent border in the first place: the devices' unique spatio-temporal digitized nature. Indeed, as the controversy over border searches of digital devices continues to "extend" into the future despite past efforts by the federal government and courts alike to assert that no level of suspicion is necessary to effectuate such searches,[174] there truly is reason to suspect that a renewed look at the issue is needed to honor travelers' (and their laptops') reasonable expectations of privacy.[175]

---

[172] *See Cotterman*, 709 F.3d at 956-957.

[173] *See supra* pp. 24-25.

[174] *Cotterman (2013)* functions as the lone exception.

[175] While the *Cotterman (2013)* court's requirement of a reasonable suspicion standard to conduct a forensic analysis of a digital device sought to protect substantial privacy interests not pursued in this note, *Cotterman*, 709 F.3d at 957, its status as the first case to articulate a "reasonable suspicion" standard to conduct a border search of a digital device illustrates that a renewed look is also (and finally) being given.