HIJACKED AT THE BORDER: Why the Government Should Have Reasonable Suspicion Before Conducting Intrusive Examinations of Our Personal Electronic Devices

Ryne Spengler[†]

[†] J.D. Candidate, Seton Hall University School of Law, 2015. I would like to thank my wife, Ashley, for all of her love and support in pursuing my dreams. Without her, none of this would be possible. I would also like to thank my family and friends for the encouragement they have given me over the years. Finally, I would like to thank Dean Erik Lillquist for his guidance and insight throughout the entire writing process, as well as the staff of *Seton Hall Circuit Review* for their help in editing.

PART I: INTRODUCTION

When a person travels across the United States border, whether by land, by air, or by sea, that person and their belongings may be subjected to a warrantless search and seizure by a border patrol agent.[1] According to the Supreme Court, these searches do not require probable cause and are reasonable by their very nature.[2] This line of reasoning makes sense, as the security at our borders is paramount,[3] especially in the wake of the September 11th attacks. Nevertheless, there has to be some line established that the government cannot cross when conducting certain border searches, particularly those involving significant privacy interests. As technology advances and the digitalization of our personal lives continues to increase, the search of personal electronic devices raises unique border security concerns, now more than ever.

In *United States v. Seljan*, the Ninth Circuit reasoned that the border search doctrine cannot stand for the idea that "at the border, 'anything goes.'"[4] Moreover, the Supreme Court raised its own concerns in *United States v. Montoya de Hernandez*, suggesting that there was a limited scope as to what could be considered "routine" customs searches and inspections.[5] The problem then becomes defining what can be considered a non-routine border search, and the level of suspicion that is required before conducting such a search.[6] While the government's interest in searches at our international borders is significant, it must still be weighed against important individual privacy interests. In performing this balancing of the interests, "the touchstone of the Fourth Amendment analysis remains reasonableness."[7]

Thus, as our lives continue to become more and more intertwined with our electronic devices, one's digital life can be seen as an extension of that person's real life, as these devices "contain the most intimate details

---

[1] 19 C.F.R. § 162.6 (2010) (stating that "All persons, baggage, and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs officer"); *see also Border Security: At Ports of Entry,* U.S. CUSTOMS AND BORDER PROTECTION (last visited Feb. 7, 2015), http://www.cbp.gov/border-security/ports-entry (stating that "U.S. Customs and Border Protection has a complex mission at ports of entry with broad law enforcement authorities tied to screening all foreign visitors, returning American citizens and imported cargo that enters the U.S. at more than 300 land, air and sea ports.").

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

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

[4] United States v. Cotterman, 709 F.3d 952, 960 (9th Cir. 2013) (quoting United States v. Seljan, 547 F.3d 993, 1000 (9th Cir. 2008)(en banc)).

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

[6] *Id.* at n.4 ("we suggest *no view* on what level of suspicion, if any, is required for nonroutine border searches") (emphasis added).

[7] *Cotterman*, 709 F.3d at 960 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985)).

of our lives."[8] Although border searches of electronic devices "have yielded evidence of illegal conduct[,]" such searches still raise a number of "significant privacy concerns.".[9]

The Fourth Circuit was the first court to address whether border searches of electronic devices require a heightened standard in *United States v. Ickes*, holding that suspicion is not necessary to perform such searches.[10] Recognizing that intrusive searches of a person's electronic devices invoke special concerns, the Ninth Circuit departed from this suspicionless standard and instead adopted the view that border agents should have at least a "reasonable suspicion" before searching a person's electronic devices.[11] The United States Supreme Court should adopt a reasonable suspicion standard to resolve this circuit split, and preserve important individual liberty interests.

Part II of this Comment provides the background of relevant sources to this debate, discussing the factual background of *United States v. Cotterman* and evolution of the border search doctrine as a whole. Part III analyzes these sources, discussing the aptness of the Ninth Circuit's decision, and highlighting where the other circuits have faltered in their analysis. Part IV concludes this Comment.

PART II: BACKGROUND

A. Factual Background of United States v. Cotterman

Howard Cotterman and his wife were crossing the United States-Mexico border in April 2007. During a primary inspection, border agents came across a hit on the Treasury Enforcement Communications System ("TECS").[12] TECS indicated to the border agent conducting the inspection that Cotterman was not only a sex offender, but possibly involved in child sex tourism as well.[13] As a result of the hit, the agents subsequently searched Cotterman's vehicle, where they found two laptops and three digital cameras.[14] A cursory search of these devices revealed that they contained both personal photographs as well as password-protected files.[15]

---

[8] *Id.* at 964.

[9] Mary Ellen Callahan, *Privacy issues in border searches of electronic devices*, U.S. DEP'T OF HOMELAND SECURITY, (October 2009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacyprivacyissuesborder_searcheselectronicdevices.pdf

[10] United States v. Ickes, 393 F.3d 501 (4th Cir. 2005).

[11] *Cotterman*, 709 F.3d at 966.

[12] *Id.* at 957.

[13] *Id.*

[14] *Id.*

[15] *Id.* at 957–58.

The border agents contacted Immigration and Customs Enforcement ("ICE") for further instruction in handling the search.[16] ICE informed the agents that the alert was part of a system that identified registered sex offenders in an effort to fight child sex tourism.[17] Due to the nature of the hit, ICE advised the agents to review any electronic devices, such as his computers and cameras, in order to discover whether Cotterman was in possession of child pornography.[18]

Although the border agents were able to view some of the files on Cotterman's computer, many of the files were still password-protected, and therefore inaccessible.[19] At this point, ICE agents were en-route to the Port of Entry, deciding to perform a more intrusive search of Cotterman's laptops when they arrived.[20] Although Cotterman initially offered to help access those files that were password-protected, the agents declined Cotterman's offer, fearing that Cotterman might delete the files, or that the computer itself was "booby trapped."[21]

The subsequent search revealed seventy-five images of child pornography on Cotterman's laptop. Notwithstanding this discovery, the password-protected files on the laptop were still inaccessible.[22] The agent who performed the search, ICE Senior Special Agent & Computer Forensic Examiner John Owen, conceded at this point that he would need Cotterman's help in order to access the protected files. Yet Cotterman never showed up to assist Agent Owen.[23] After another attempt to gain his assistance, Cotterman responded that the computer had multiple users. Cotterman informed Agent Owen that he would need to contact these other people to retrieve their passwords.[24]

Despite Cotterman's lack of assistance, Agent Owen finally opened the files on April 11. Access to these additional files revealed another 378 images of child pornography. The vast majority of these images were of the same girl over a two-to-three-year period, and many depicted Cotterman sexually molesting other children as well.[25] A continued search over the next few months revealed hundreds more files, including images, stories and videos of children.[26] When Cotterman's case went to trial, the

---

[16] *Id.* at 958.
[17] *Cotterman*, 709 F.3d at 958.
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Cotterman*, 709 F.3d at 958.
[22] *Id.*
[23] *Id.*
[24] *Id.* at 958–59.
[25] *Id.* at 959.
[26] *Cotterman*, 709 F.3d at 959.

government "sought a broad ruling that no suspicion of any kind was required" to perform these searches on Cotterman's laptops.[27]

B. Evolution of the Border Search Doctrine

The Fourth Amendment of the United States Constitution guarantees that "[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 . . . ."[28] When a search occurs, it implicates this right so long as the individual has a subjective expectation of privacy, and that expectation is one that society objectively recognizes as reasonable.[29] Thus, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[30]

While obtaining a judicial warrant may generally fulfill this requirement,[31] a search may, nevertheless, be deemed reasonable if it falls within a specific exception to the warrant requirement.[32] These exceptions include: exigent circumstances,[33] automobile searches,[34] inventory searches,[35] consent searches,[36] searches in plain view,[37] *Terry* "Stops and Frisks,"[38] searches incident to arrest,[39] and occasions where special needs

---

[27] *Id.*

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

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

[30] Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

[31] Vernonia School Dist. 47JA v. Acton, 515 U.S. 646, 653 (1995).

[32] Riley v. California, —- U.S. ——, 134 S.Ct. 2473, 2482 (2014).

[33] *See, e.g., Brigham City*, 547 U.S. 398 (allowing a warrantless search when there is an "objectively reasonable" belief that a person is seriously injured or threatened with such injury); Michigan v. Tyler, 436 U.S. 499, 510 (1978)(reasoning that warrantless entry should be allowed to put out a fire and investigate its cause).

[34] *See* California v. Acevedo, 500 U.S. 565, 574-75 (1991)(holding that police may, without a warrant, search an automobile and the containers within it wherever they have probable cause to believe the contraband may be contained).

[35] *See* Florence v. Board of Chosen Freeholders, —- U.S. ——, 132 S.Ct. 1510, 1517 (2012)(noting that deference is given to correctional officers when performing inventory searches of inmates); South Dakota v. Opperman, 428 U.S. 364, 372 (1976)(applying the inventory search exception to impounded vehicles).

[36] *See, e.g.,* Schneckloth v. Bustamonte, 412 U.S. 218 (1973)(reasoning that voluntary consent to a search eliminates the warrant requirement).

[37] *See* Minnesota v. Dickerson, 508 U.S. 366, 375 (1993)(stating that the exception applies "if police are lawfully in a position from which they view an object, if its incriminating character is immediately apparent, and if the officers have a lawful right of access to the object.").

[38] Terry v. Ohio, 392 U.S. 1, 21 (1968)(stating that objective reasonableness is the proper inquiry in these types of searches).

[39] *See* Chimel v. California, 395 U.S. 752, 762 (1969)(reasoning that the two justifications for this type of warrantless search are for officer safety and to prevent the destruction or concealment of evidence).

allow for a search to be performed without a warrant.[40] The Supreme Court has specifically justified warrantless searches at the United States borders under this latter-most category.

The United States Supreme Court has long upheld the constitutionality of unwarranted border searches.[41] As such, the Court has specifically recognized that, "[t]ravelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in."[42] As part of this longstanding tradition, the Court reached a landmark decision in 1977 case *United States v. Ramsey*.[43] In *Ramsey*, the Court expanded the idea of a border search exception by addressing the reasonableness of such searches. The Court reasoned that:

[b]order searches . . . from before the adoption of the Fourth Amendment, have been considered to be "reasonable" by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause.[44]

Such a broad exception, however, yields complications when applied to more intrusive border searches. In *United States v. Montoya de Hernandez*, the Court was charged with deciding what level of intrusiveness could negate the presumption of reasonableness.[45]

In *Montoya de Hernandez*, customs officials performed a rectal examination on the defendant, discovering that she had been smuggling a balloon filled with cocaine in her alimentary canal.[46] The defendant argued that such a search was unreasonable. The Supreme Court disagreed, noting that "[w]hat is reasonable depends upon all of the circumstances surrounding the search or seizure and the nature of the

---

[40] *See* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 624 (1989)(reasoning that "[i]n limited circumstances, where the privacy interests implicated by the search are minimal, and where an important government interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion, a search may be reasonable despite the absence of such suspicion."); New Jersey v. T.L.O., 469 U.S. 325 (1980)(applying the special needs doctrine to searches in schools, reasoning that a "less exacting" standard than probable cause is required).

[41] *See* Boyd v. United States, 116 U.S. 616 (1886); *see also* Carroll v. United States, 267 U.S. 132 (1925).

[42] Carroll v. United States, 267 U.S. 132, 154 (1925).

[43] United States v. Ramsey, 431 U.S. 605 (1977)(discussing the constitutionality of a warrantless search involving an individual's international letter-class mail).

[44] *Id.* at 619.

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

[46] *Id.* at 535.

search or seizure itself."[47] The Court drew on the distinction between ordinary searches and seizures, and those that occur at international borders.[48] The Court reasoned that "the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal."[49] While the Court's holding did not require that border patrol agents have probable cause, as in the case of normal searches, *Montoya de Hernandez* opened the door to the suggestion that certain types of border searches will not be deemed reasonable simply due to the fact that they occurred at a United States border.

The Supreme Court further distinguished the varying levels of border searches in *United States v. Flores-Montano,* when customs officials seized marijuana from the defendant's gas tank.[50] As part of their search, the customs officials "remov[ed] and disassembl[ed] the tank" to discover the defendant's contraband.[51] The Ninth Circuit, citing *Montoya de Hernandez*, had argued that the customs officials needed reasonable suspicion before their search of the tank.[52] The Supreme Court rejected this application of a reasonable suspicion standard, instead asserting that:

> [R]easons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person – dignity and privacy interests of the person being searched – simply do not carry over to vehicles. Complex balancing tests to determine what is a "routine" search of a vehicle, as opposed to a more "intrusive" search of a person, have no place in border searches of vehicles.[53]

While the Court thus alluded to the fact that a heightened standard might be required when dealing with more "highly intrusive searches,"[54] it has yet to address the distinction between those border searches that do and those that do not require reasonable suspicion.

---

[47] *Id.* at 537.
[48] *Id.* at 537–39.
[49] *Id.* at 541.
[50] United States v. Flores-Montano, 541 U.S. 149 (2004).
[51] *Id.* at 149.
[52] *Id.* at 152.
[53] *Id.* at 152.
[54] *Id.*

C. The Fourth Circuit's Findings in United States v. Ickes

The Fourth Circuit was the first circuit to directly examine the question of whether any level of suspicion was required for border searches of personal electronic devices. In *United States v. Ickes*,[55] the defendant was convicted of transporting child pornography across a United States border due to the images found on his computer.[56] When Ickes came to the United States-Canada border, he claimed to be on his way home from vacation, but the primary inspector at the border was wary of this assertion. The inspector's suspicions came about because the van that Ickes was traveling in seemed to contain "everything he own[ed]."[57] The inspector therefore referred Ickes to a secondary inspection station.[58]

During the search at the secondary station, one of the agent's "suspicions were raised" after viewing a video that seemingly focused on "a young ball boy at a tennis match".[59] With this heightened level of awareness, the agent commenced a fuller search of the defendant's van.[60] After searching the vehicle, the agent and his colleague discovered drugs and child pornography, as well as a warrant for Ickes' arrest.[61] The agents confiscated Ickes' computer, along with "75 disks containing additional child pornography."[62] At trial, Ickes filed a motion to suppress the evidence found on his computer and these disks, claiming they were obtained through a warrantless search in violation of his rights under the First and Fourth Amendments of the United States Constitution.[63]

As part of its analysis, the Fourth Circuit looked to the language of 19 U.S.C.A. §1581(a). This statute provides, in relevant part:

> Any officer of the customs may at any time go on board of any vessel or vehicle at any place in the United States or within the customs waters . . . or at any other authorized place . . . and examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and any person, trunk, package or cargo on board.[64]

---

[55] United States v. Ickes, 393 F.3d 501 (4th Cir. 2005).
[56] *Id.* at 502.
[57] *Id.*
[58] *Id.*
[59] *Id.* Although the court ultimately rejects a standard that would necessitate any raised level of suspicion for a search of electronic devices, it is interesting to note here that the circumstances surrounding this search probably would have met a reasonable suspicion standard regardless.
[60] *Ickes*, 393 F.3d at 503.
[61] *Id.* at 503.
[62] *Id.*
[63] *Id.*
[64] 19 U.S.C.A. §1581(a) (1954).

The defendant argued that because the statute contained no explicit reference to electronic equipment, the search of his computer and disks were unsupported by the statutory authority.[65] The court rejected this argument, focusing on the statute's use of the term "cargo" to support its findings.[66]

The court noted that "cargo" was defined by Black's Law Dictionary as those "goods transported by a vessel, airplane, or vehicle."[67] Because the computer and disks were "cargo" within this meaning and because it was "undisputed that [these items] were being transported by [Icke's] vehicle" at the time that the search was conducted, the search was authorized by § 1581.[68] The court likewise found that the use of the word "any" five times in the statute indicated that the 19 U.S.C.A. §1581(a) should be construed broadly.[69] Furthermore, the court reasoned that past cases have also supported this tendency to read §1581 expansively.[70] Any other reading, according to the court, would "undermine the long-standing practice of seizing goods at the border even when the type of good is not specified in the statute."[71]

Ickes also argued that the search of his computer and disks was in violation of his rights under the United States Constitution.[72] He claimed that despite the government's interests of protecting the borders, these interests did not outweigh his own privacy interests.[73] The court disagreed, focusing on the Supreme Court's rationale in *Flores-Montano* that:

> [t]he government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, we have stated that searches made at the border . . . are reasonable simply by virtue of the fact they occur at the border.[74]

This government interest in protecting and patrolling the border substantially outweighed whatever privacy interest Ickes claimed to have in his electronic devices. The authority under the border search doctrine, the court explained, "has a history as old as the Fourth Amendment itself."[75]

---

65 United States v. Ickes, 393 F.3d 501, 504 (4th Cir. 2005).
66 *Id.*
67 *Id.* (quoting BLACK'S LAW DICTIONARY 226 (8th ed. 2004).
68 *Id.*
69 *Id.*
70 *Ickes*, 393 F.3d at 505.
71 *Id.* at 504.
72 *Id.* at 505.
73 *Id.* at 506.
74 *Id.* at 505 (quoting United States v. Flores-Montano, 541 U.S. 149 (2004)).
75 *Ickes*, 393 F.3d at 505. (quoting United States v. Ramsey, 431 U.S. 606, 619 (1977)).

The Fourth Circuit likewise refused to create an exception to the border search doctrine, grounded in the First Amendment.[76] Ickes argued, unsuccessfully, that the content on his computer and disks were "expressive" and therefore were protected by his First Amendment rights.[77] In rejecting Ickes' contention, the court suggested that the proposition would create "significant headaches for those forced to determine the scope" of the exception.[78] Additionally, it would force border agents to decide "on their feet" what material is covered by the First Amendment. After making this determination, and if covered by the exception, the agents would then have to decide whether or not probable cause exists before they can conduct a search.[79] The court reasoned that "[t]he essence of border search doctrine is a reliance upon the trained observations and judgments of customs officials, rather than upon constitutional requirements applied to the inapposite context of this sort of search."[80]

PART III: ANALYSIS

A. The Unique Characteristics of Personal Electronic Devices

Intrusive searches of a person's electronic devices are inherently different from searches performed on other belongings. By their very nature, these devices contain significantly more information about an individual's personal life than any other type of luggage that one may carry at an international border. In fact, "[e]very computer is akin to a vast warehouse of information."[81] The types of data contained on computers run the gamut from the impersonal to the highly personal. With the rapid advances of modern technology, this range is ever increasing.[82] Notwithstanding this fact, computer users might not even know about much of the information that is stored on these devices, much less be able to control it.[83] Much of what a person believes they have deleted or

---

[76] *Id.* at 506.
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.* at 507.
[81] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (Dec. 2005).
[82] *See, e.g.,* Farhad Manjoo, *Apple Watch Review: Bliss, but Only at a Steep Learning Curve*, N.Y. TIMES (Apr. 8, 2015), http://www.nytimes.com/2015/04/09/technology/personaltech/apple-watch-bliss-but-only-after-a-steep-learning-curve.html?_r=0/ (reviewing the Apple's revolutionary smartwatch concept, and explaining that "the most exciting thing about the Apple Watch isn't the device itself, but the new tech vistas that may be opened by the first mainstream wearable computer.")
[83] *Id.*

removed remains on the device in some form, despite the attempted erasure, "mak[ing] it impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel."[84]

When a person is subjected to an extensive search of one's digital life, absent any sort of reasonable suspicion, a person is likely to feel a level of violation approaching that of a strip search. Such a search exposes the very intimate details of that person's life, equivalent more to a line-by-line combing through one's diary than to the impersonal search of a car.[85] Furthermore:

> [u]nlike searches involving a reassembled gas tank or small hole in the bed of a pickup truck, which have minimal or no impact beyond the search itself—and little implication for an individual's dignity and privacy interests—the exposure of confidential and personal information has permanence. It cannot be undone. Accordingly, the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property.[86]

Due to these stark differences, the data that is collected after an intrusive forensic search should not be conflated with other types of luggage that a person carries across the border.[87] This information is not mere luggage, but rather an extension of the person.[88] It is this interconnection between the person and the device that necessitates a heightened standard before conducting an intrusive search.

Not only is the nature of the search results inherently different from that which other border searches yield, but the nature of the search itself similarly differs. For instance, "the computer search process tends to be more labor intensive and *thorough* than the physical search of a home."[89] If this contention is correct, it follows that such searches cannot be

---

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

[85] *Id.* at 963.

[86] *Id.* at 966 (citations omitted).

[87] *See, e.g.*, Christine A. Coletta, *Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment*, 48 B.C. L. REV. 971, 1001 (Sept. 2007)("Because a computer can contain vast amounts of data that a passenger is unlikely to pack for a vacation or trip, a search through its hard drive is not analogous to looking through a person's luggage, wallet, or automobile. It is much more personal, and implicates dignity and privacy interests that should contribute to a finding that a laptop search is intrusive").

[88] John W. Nelson, *Border Confidential: Why Searches of Laptop Computers at the Border Should Require Reasonable Suspicion*, 31 AM. J. TRIAL ADVOC. 137, 140 (2007).

[89] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 544 (Dec. 2005)(emphasis added).

classified as "routine" under *Montoya de Hernandez*. It is for these reasons, among others, that the *Cotterman* court applied a reasonable suspicion standard to border searches of personal electronic devices.[90]

B. The Ninth Circuit's Findings in United States v. Cotterman

Prior to its decision in *Cotterman*, the Ninth Circuit had developed its own understanding of the border search doctrine through prior case law. In *United States v. Ramos-Saenz*, the court attempted to define what the Supreme Court meant by a "nonroutine" border search, reasoning that "a border search goes beyond the routine only when it reaches the degree of intrusiveness present in a strip search or a body cavity search."[91] In fashioning this definition, similar to the Supreme Court's distinction in *Flores de Montano*, the court recognized that there was some level of intrusiveness that would bring a border search beyond that which was simply "routine," and thus reasonable per se.[92]

The Ninth Circuit, however, initially declined to extend this reasoning when it first examined the question of whether the doctrine would apply to personal electronic devices in *United States v. Arnold*.[93] In *Arnold*, the court specifically held that "reasonable suspicion is not needed to search a laptop or other personal electronic storage devices at the border."[94] Despite this holding, the unique characteristics of personal electronic devices themselves caused the court to reexamine the doctrine's application to searches of these devices five years later, and flatly reject that reasoning when it decided *United States v. Cotterman*.[95]

In *Cotterman*, the Ninth Circuit analyzed Supreme Court precedent in order to reach its ultimate conclusion that reasonable suspicion is necessary for extensive border searches of personal electronic devices.[96] The court began by examining the subject of searches and seizures at United States borders in general. "The broad contours of the scope of searches at our international borders are rooted in 'the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country.'"[97] The court stated that the language of *Ramsey* led to the development of the rule that border searches are reasonable purely because they occur at the border.[98] Nevertheless, the

---

[90] United States v. Cotterman, 709 F.3d 952, 962–68 (9th Cir. 2013).
[91] United States v. Ramos-Saenz, 36 F.3d 59, 61 (9th Cir. 1994).
[92] *Id.*
[93] United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008).
[94] *Id.* at 1008.
[95] *Cotterman*, 709 F.3d at 962.
[96] *Id.* at 960.
[97] *Id.* (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977)).
[98] *Id.*

court asserted that this was not the end of the matter. The court limited *Ramsey*, proclaiming that the holding "does not mean . . . that at the border 'anything goes.'"[99] Instead, the key factor remains the "reasonableness" of the search, which depends, in turn, on the totality of the circumstances.[100]

The court recognized that Officer Alvarado's initial search of Cotterman's laptop did not require reasonable suspicion because it was akin to a cursory scan of a package.[101] The court acknowledged that, "[h]ad the search of Cotterman's laptop ended with [the initial search, it] would be inclined to recognize it was reasonable even without particularized suspicion."[102] But the "reasonableness" of the forensic examination was, in the court's view, a far more difficult issue to determine.[103]

The court began by declining to treat the forensic examination of Cotterman's laptop as a so-called "extended border search," which require particularized suspicion in order to proceed.[104] Judge Smith's dissent argued that the forensic examination would qualify as such a search because it occurred around one hundred and seventy miles from the border and several days after Cotterman attempted to enter the country.[105] The majority, however, rejected this proposition.[106] Rather, the majority reasoned that the doctrine was "best confined to cases in which, after an apparent border crossing or functional entry, an attenuation in the time or the location of conducting a search reflects that the subject has regained an expectation of privacy."[107] In this case, although Cotterman was allowed to leave the inspection station, his laptop never left the possession of the border agents.[108] Therefore, Cotterman never regained the expectation of privacy recognized by the extended border search doctrine.[109]

The court similarly disregarded the argument that the forensic examination would qualify as a functional border search.[110] This doctrine involving searches at the "functional equivalent" of United States borders,

---

[99] *Id.* (quoting United States v. Seljan, 547 F.3d 993, 1000 (9th Cir. 2008)(en banc)).
[100] *Cotterman*, 709 F.3d at 960 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985)).
[101] *Id.* (citing United States v. Arnold, 533 F.3d 1003, 1009 (9th Cir. 2008)).
[102] *Id.* at 961.
[103] *Id.*
[104] *Cotterman*, 709 F.3d at 961.
[105] *Id.* at 962 (discussing Judge Smith's dissenting opinion).
[106] *Id.*
[107] *Id.*
[108] *Id.* at 961.
[109] *Cotterman*, 709 F.3d at 961.
[110] *Id.*

the court reasoned, was not applicable in Cotterman's case because the search performed was initiated at the actual border.[111] By refusing to classify the forensic examination as either an extended border search or a functional border search, the court adopted its own standard as it applied to the search of Cotterman's computers. The court asserted that "the comprehensive and intrusive nature" of the forensic examination necessitated a standard of reasonable suspicion.[112]

To justify the adoption of a heightened standard, the Ninth Circuit looked to the Supreme Court's decision in *United States v. Flores-Montano*.[113] The Ninth Circuit asserted that *Flores-Montano* stood for the proposition that the reasonableness requirement of the Fourth Amendment should control border searches.[114] Thus, the Ninth Circuit proclaimed that such a requirement was necessary, particularly in cases where "searches of property are so destructive, particularly offensive, or overly intrusive in the manner in which they are carried out."[115] The court argued that although the Supreme Court has dealt with a number of border cases over the past thirty years, none have been instructive as to when a search is "particularly offensive."[116] The issue first appeared in *United States v. Ramsey*,[117] but the Court reserved judgment.[118] Eight years later, the Court had occasion to revisit the issue in *United States v. Montoya de Hernandez*,[119] where the Court stated that such suspicion was necessary for those searches that went "beyond the scope of a *routine* customs search and inspection."[120] Thus, although the Supreme Court ultimately rejected the privacy claim in *Flores-Montano*, the Ninth Circuit reasoned that the Court's increased focus on highly intrusive searches, going beyond those that are simply "routine," supported the establishment of a reasonableness standard in certain situations.[121]

After laying the foundation for a reasonableness requirement, the Ninth Circuit turned its attention to the privacy interests connected to one's personal electronic devices.[122] The court asserted that cases like

---

111 *Id.*

112 *Id.* at 962.

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

114 United States v. Cotterman, 709 F.3d 951, 963 (9th Cir. 2013).

115 *Id.* (quoting United States v. Flores-Montano, 541 U.S. 149, 152, 154 n.2, 155-56 (2004))(internal quotation marks omitted).

116 *Id.*

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

118 *Cotterman*, 709 F.3d at 963.

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

120 *Id.* at 540–41 (emphasis added).

121 United States v. Cotterman, 709 F.3d 951, 963–64 (9th Cir. 2013)(quoting United States v. Flores-Montano, 541 U.S. 149, 152 (2004)).

122 *Id.* at 964.

Cotterman's involved the implication of "substantial personal privacy interests."[123] The court reasoned that "[t]he private information individuals store on digital devices – their personal 'papers' in the words of the Constitution – stands in stark contrast to the generic and impersonal contents of a gas tank."[124] The court argued that there were several key differences between personal electronic devices and other luggage that could constitute "cargo."[125] For instance, the storage capability of traditional luggage does not come anywhere close to the amount that one can store on electronic devices.[126]

Furthermore, electronic devices "contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails."[127] The court used this particular characteristic to analogize electronic devices to the Fourth Amendment's guarantee of a person's right to be secure in their "papers."[128] The court asserted that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[129]

The court further distinguished between traditional luggage and the files that are stored on one's personal electronic device, by exploring a person's decision-making process in deciding what kinds of "cargo" to carry with him or her.[130] While a person can decide what to pack in his or her traditional luggage, the process is not as simple for electronic devices. The court reasoned that while a person is capable in selecting the physical items that he or she is travelling with, that same person cannot merely remove files on their computer because they are impractical to travel with.[131] Furthermore, "the volume and often intermingled nature of the files" and the fact that "[i]t is also a time-consuming task that may not even effectively erase the files" led the court to dispel any suggestion that a person could simply not carry certain files with them.[132] Even when one attempts to delete these files, they may still be retrieved.[133] "It is as if a search of a person's suitcase could reveal not only what the bag contained on the current trip, but everything it had carried."[134] Thus, the court

---

123 *Id.*
124 *Id.*
125 *Id.*
126 *See, e.g.*, Kerr, *supra* note 89 at 542.
127 United States v. Cotterman, 709 F.3d 951, 964 (9th Cir. 2013).
128 *Id.* (citing U.S. Const. amend IV).
129 *Id.* at 965 (quoting Kyllo v. United States, 533 U.S. 27, 33-34 (2001)).
130 *Id.*
131 *Id.*
132 *Cotterman*, 709 F.3d at 965.
133 Kerr, *supra* note 89 at 542.
134 *Id*.

reasoned that there is an inherent difference in the selection process between what a person carries in a personal electronic device versus any other typical piece of luggage.

In recognizing these unique characteristics of personal electronic devices, the court explained its reasoning behind advancing a heightened standard for these types of border searches. The court asserted that it was not advancing a standard that would make these devices completely "off limits" to border agents, but rather it was ensuring that if such searches were to take place, they should be held to a standard of reasonableness.[135] The court ultimately asserted that "[i]nternational travelers certainly expect that their property will be searched at the border.

What they do not expect is that, absent some particularizes suspicion, agents will mine every last piece of data on their devices or deprive them of their most personal property for days."[136] The court, borrowing its definition of reasonable suspicion from *United States v. Cortez*,[137] concluded that the determination of whether or not a search is reasonable should be made in light of the totality of the circumstances.[138] Notwithstanding this reasoning, the court nevertheless found that the border agents had reasonable suspicion to search Cotterman's laptops.[139]

In reaching its ultimate conclusion, the court asserted that Cotterman's past child molestation conviction, alone, would not be enough to give rise to the suspicion necessary to conduct an intrusive computer forensic examination.[140] Similarly, the court rejected the argument that the existence of password-protected files, alone, would be enough for reasonable suspicion.[141] Because it is commonplace for persons not involved in criminal activity to protect their files, the court found password protection itself to be "ubiquitous."[142]

Nevertheless, when analyzed in light of a totality of the circumstances, the court found the aforementioned indicia to weigh in

---

[135] *Id.* at 966.

[136] *Id.* at 967 (citing United States v. Ramos-Saenz, 36 F.3d 59, 61 n. 3 (9th Cir. 1994)).

[137] United States v. Cortez, 449 U.S. 411, 417–19 (1981)("a particularized and objective basis for suspecting the particular person stopped of criminal activity").

[138] *Cotterman*, 709 F.3d at 968 (citing United States v. Cortez, 449 U.S. 411, 417 (1981)).

[139] *Id.* at 968.

[140] *Id.* (quoting Burrell v. McIlroy, 464 F.3d 853, 858 n. 3 (9th Cir. 2006)) ("Although a prior criminal history cannot alone establish reasonable suspicion . . . it is permissible to consider such a fact as part of the total calculus of information in th[at] determination [ ].").

[141] *Id.*

[142] *Id.*

favor of a finding of reasonableness.[143] The following factors, taken together, ultimately supported the court's assertion that the border agents had reasonable suspicion when conducting both the initial search and the comprehensive forensic examination of Cotterman's laptop: Cotterman's TECS alert; Cotterman's prior conviction for child molestation; Cotterman's frequent travels; the fact that Cotterman was attempting to cross the border from a country known for sex tourism (Mexico); Cotterman's collection of electronic equipment; the fact that Cotterman had password-protected his files; and the parameters of the system that was used to identify registered sex offenders.[144] Thus, although the Ninth Circuit ultimately adopted a new standard for border searches of electronic devices, the border agents who searched Cotterman's laptop had the requisite level of suspicion for performing a comprehensive forensic examination.

C. A Step In The Right Direction: The United States Supreme Court's Decision in Riley v. California

Less than a year after the Ninth Circuit handed down its decision in *Cotterman*, the United States Supreme Court granted certiorari in two companion cases whose effects have potential to change the judicial landscape surrounding warrantless searches of electronic devices.[145] In the first case, David Riley had been pulled over for driving with expired tags.[146] After learning that Riley was also driving with a suspended license, the officer impounded Riley's car and arrested Riley after an inventory search turned up two handguns under the car's hood.[147] An officer then searched Riley incident to arrest, seizing Riley's cell phone in the process.[148] The officer looked through the phone, noticing the letters "CK" appear multiple times, a label which he believed to stand for the moniker "Crip Killers," used to describe members of the Bloods gang.[149] Thus, two hours later, a detective further examined the phone's content, looking for more evidence of gang activity.[150] This search ultimately

---

[143] *Cotterman*, 709 F.3d at 968. ("Collectors of child pornography can hardly be expected to clearly label such files and leave them in readily visible and accessible sections of a computer's hard drive, particularly when they are traveling through border crossings, where individuals ordinarily anticipate confronting at least a cursory inspection.").

[144] *Id.* at 968–70.

[145] Riley v. California, 571 U.S. ——, 134 S.Ct. 999 (2014); United States v. Wurie, 571 U.S. ——, 134 S.Ct. 999 (2014).

[146] Riley v. California, —- U.S. ——, 134 S.Ct. 2473, 2480 (2014).

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] *Id.*

turned up videos and photographs which linked Riley to the Bloods gang and a car that had been involved in a shooting a few weeks earlier.[151]

In the companion case, a police officer witnessed Brima Wurie sell drugs from his car.[152] After Wurie was arrested and brought to the police station, officers seized two cell phones from Wurie's person.[153] The officers noticed that the phone was receiving phone calls from the same number, identified as "my house" on the phone's external screen.[154] After opening the phone and accessing its call log, the officers traced the number associated with "my house" back to an apartment building.[155] Upon searching the apartment, pursuant to a warrant, the officers found and seized "215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash."[156] Wurie was subsequently charged based on this evidence.[157]

The Supreme Court began the opinion by reflecting on its own precedent regarding searches incident to arrest.[158] More relevant to the present inquiry, however, the Court then highlighted the changes that advancing technology bring to the Fourth Amendment analysis.[159] The Court reasoned that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[160] Thus, like the Ninth Circuit's analysis in *Cotterman*, the Supreme Court was similarly forced to focus its analysis on the balance between an individual's privacy and the promotion of government interests.[161] In doing so, the Court refused to adopt a mechanical approach to its interpretation of Fourth Amendment precedent.[162] Ultimately, the Court decided that, due to the inherent differences between a physical search and a search of cell phone information, officers must secure a warrant before conducting such an intrusive search.[163]

---

151 *Riley*, 134 S.Ct. at 2480.
152 *Id.* at 2481.
153 *Id.*
154 *Id.*
155 *Id.*
156 *Riley*, 134 S.Ct. at 2481.
157 *Id.*
158 *Id.* at 2482–84.
159 *Id.* at 2484 (reasoning that the phones' technology would have been inconceivable when *Chimel* and *Robinson* were decided).
160 *Id.*
161 *Riley*, 134 S.Ct. at 2484.
162 *Id.*
163 *Id.*

D. Why the Ninth Circuit's Reasonable Suspicion Standard Should be Adopted in Light of Riley

As the Ninth Circuit announced in its decision, "[a] person's digital life ought not be hijacked simply by crossing a border."[164] While the Fourth Circuit's findings in *Ickes* are persuasive, these findings do not override what the Supreme Court has established in its border search doctrine precedent.[165] As the doctrine itself has developed, there has been more reluctance on the Court's part to follow the blanket rule set forth in *Ramsey*.[166]

There are stark differences between opening someone's mail and digging through personal files stored on one's computer. For instance, "[e]lectronic devices often retain sensitive and confidential information far beyond the perceived point of erasure, notably in the form of browsing histories and records of deleted files."[167] These files cannot be equated to a traveler's usual "cargo," as the *Ickes* court noted. Computers themselves work through the interplay of hardware and software components.[168] A computer's hardware includes "the parts of a computer that you can see and touch, including the case and everything inside it."[169] While this aspect of a computer easily fits the definition adopted by the Fourth Circuit, the computer's software and files are more difficult to classify as "goods transported by a vessel, airplane, or vehicle."[170] As opposed to a computer's hardware, its "[s]oftware refers to the instructions, or programs, that tell the hardware what to do."[171] While software may be seen as "goods" on one level, the differences inherent between the two components should be taken into account in the larger analysis.

Furthermore, computers are multi-faceted devices. A person's computer therefore has endless possibilities in the types of uses and information associated with it. "In the workplace, many people use computers to keep records, analyze data, do research, and manage projects. At home, [they] can use computers to find information, store pictures and music, track finances, play games, and communicate with others—and

---

164 United States v. Cotterman, 709 F.3d 951, 965 (9th Cir. 2013).

165 *See supra,* Part II.B.

166 *See generally* United States v. Montoya de Hernandez, 473 U.S. 531 (1985).

167 *Id.*

168 *Introduction to Computers*, WINDOWS, (last visited Feb. 7, 2015), http://windows.microsoft.com/en-us/windows/introduction-to-computers#1TC=windows-7.

169 *Id.*

170 United States v. Ickes, 393 F.3d 501, 504 (4th Cir. 2005)(quoting BLACK'S LAW DICTIONARY 226 (8th ed. 2004).

171 *Introduction to Computers, supra* note 168.

those are just a few of the possibilities."[172] In order for a border agent to perform a search with the level of intrusiveness that was found in *Cotterman*, it should follow that there was some amount of suspicion on their part before the search was conducted. Otherwise, virtually every aspect of a person's digital life will be available for inspection at the will of those working at the United States border.

Since *Ramsey*, Supreme Court precedent has displayed an ever-increasing awareness that the border search doctrine is more flexible than it appears on its face. While the U.S. Department of Homeland Security ("DHS") is authorized to conduct the "inspection, examination, and search of vehicles, persons, baggage and merchandise . . . to ensure compliance with any law or regulation enforced or administered by DHS,"[173] the Court has recognized certain types of searches to necessitate a heightened standard. Such was the case in *Montoya de Hernandez*, in which the Court discussed the need for reasonableness before a border agent performs a rectal examination.[174] While searching a person's computer is not the equivalent of a search of a person's alimentary canal, the emphasis the Court placed on the intrusive nature of the search is nevertheless instructive.[175]

Even when a search is not particularly offensive, "[f]or those pulled aside for a secondary inspection . . . the experience can be distressing, resulting in a missed connecting flight, a prolonged interrogation, and . . . the loss of a laptop necessary for [his or her] livelihood."[176] Distress related to such searches only increases when the search becomes more intrusive. Around five thousand people were subjected to electronic media searches between October 1, 2012 and August 31, 2013, which amounts to about fifteen such searches a day.[177] If these numbers continue to increase without any guidance or restraint, intrusive computer examinations will *become* the types of routine searches allowed by *Montoya de Hernandez*. This trend is particularly alarming given the privacy concerns implicated by border searches of electronic devices.

---

[172] *Introduction to Computers, supra* note 168.

[173] *Privacy Impact Assessment for the Border Searches of Electronic Devices*, U.S. DEP'T OF HOMELAND SECURITY, at 2 (Aug. 25, 2009).

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

[175] *See id.* (reasoning that "[t]he 'reasonable suspicion' standard has been applied in a number of contexts and effects a needed balance between private and public interests when law enforcement officials must make a limited intrusion on less than probable cause.").

[176] Susan Stellin, *The Border Is a Back Door for U.S. Device Searches*, N.Y. TIMES, (Sept. 9, 2013), http://www.nytimes.com/2013/09/10/business/the-border-is-a-back-door-for-us-device-searches.html?
pagewanted=2&_r=0&hp.

[177] *Id.*

Although addressing a separate exception to the Fourth Amendment's warrant requirement, *Riley* provides valuable insight into how this issue should be viewed moving forward across Fourth Amendment jurisprudence as a whole. As the Supreme Court recognized in *Riley*, personal technological devices, such as cell phones, "place vast quantities of personal information literally in the hands of individuals."[178] While the Court acknowledged the tremendous government interest in that information, particularly given concerns regarding the potential loss of evidence, it also realized that there are other ways to alleviate those concerns.[179] "If 'the police are truly confronted with a "now or never situation.'" – for example, circumstances suggesting that a defendant's phone will be the target of an imminent remote-wipe attempt – they may be able to rely on exigent circumstances to search the phone immediately."[180]

By contrast, the privacy concerns implicated in a cell phone search are far greater than those of physical items that the Supreme Court has addressed in the past.[181] The inherent differences between the two types of items are apparent. "Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read – nor would they have any reason to attempt to do so."[182] Thus, the limitations that exist with searches of physical containers do not apply to personal electronic devices, as devices like cell phones can store vast amounts of data that would be impractical, if not impossible, to carry on the person physically.[183] Moreover,

> [t]he fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone,

---

[178] Riley v. California, —- U.S. ——, 134 S.Ct. 2473, 2485 (2014).

[179] *Id.* at 2485–87 (explaining how the *Chimel* rationales of officer safety and destruction of evidence are inapplicable to cell phone data).

[180] *Id.* at 2487 (quoting Missouri v. McNeely, 569 U.S. ——, 133 S.Ct. 1552, 1561–62 (2013)(citations omitted)) .

[181] *Id.* at 2488–89 (comparing a cell phone to a wallet or a purse "is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.").

[182] *Id.* at 2489.

[183] *Riley*, 134 S.Ct. at 2489 (citing Orin S. Kerr, *Foreword: Accounting For Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 404 (2013).

> even though people would be unlikely to carry such a variety of information in physical form.[184]

Searches of electronic devices would also allow access to types of information that a physical search would never reveal.[185] Such information may not only be on the device itself, but stored remotely on servers through the ever-increasing use of "cloud computing."[186]

As the Court recognized, albeit with a particular focus on cell phones in the search incident to arrest context, the unique characteristics of one's personal electronic devices require that there be some sort of shield against suspicionless searches, given the tremendous privacy interests at stake.[187] That is not to say that security at our nation's borders is not paramount.[188] Rather, there are times when the government must realize that the nature of certain types of searches goes too far when weighed against an individual's privacy interests.[189] An intrusive search of one's personal electronic devices without at least a minimal requirement of reasonable suspicion is one of those times. When an "exhaustive forensic search of a copied laptop hard drive" is performed, it "intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border."[190] Such a search should be held to the reasonableness requirement of the Fourth Amendment, rather than falling under the general exemption of the border search doctrine.[191] The reasonable suspicion standard advanced by the Ninth Circuit should, thus, be adopted by the Supreme Court in order to resolve this circuit split.

---

[184] *Id.* at 2493; *see also id.* at 2489 (describing the variety of information that a cell phone search could reveal about an individual).

[185] *Id.* at 2490 (stating that "[a]n Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns – perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been.").

[186] *Id.* at 2491.

[187] *See Riley*, 134 S.Ct. at 2494–95 (stating that "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."); *see also* U.S. Const. amend IV.

[188] United States v. Flores-Montano, 541 U.S. 149, 153 (2004).

[189] *See*, *e.g.,* Hugo Martin, *Controversial full-body scanners to be removed from airports*, L.A. TIMES (Jan. 18, 2013), http://articles.latimes.com/2013/jan/18/business/la-fi-tsa-rapiscan-20130119; *see also TSA gets rid of full-body scanners at US airports*, FOX NEWS (May 31, 2013), http://www.foxnews.com/politics/2013/05/31/tsa-gets-rid-full-body-image-scanners-at-us-airports/.

[190] United States v. Cotterman, 709 F.3d 951, 966 (9th Cir. 2013).

[191] *See* United States v. Saboonchi, 2014 U.S. Dist. LEXIS 102261 at *13 (D. Md. July 28, 2014)(reasoning that while *Riley* is inapplicable to border searches, the court still held that "[a]n invasive and warrantless border search may occur on no more than reasonable suspicion . . . .").

PART IV: CONCLUSION

With the growth and development of technology, the law must evolve to reflect the changing times. No longer should courts be able to hold onto strict applications of rules that were created before certain technologies came into existence. The border search doctrine is one of those rules that must develop accordingly. The reasonable suspicion standard adopted by the Ninth Circuit in *United States v. Cotterman* properly addresses the privacy concerns associated with one's digital life, while maintaining the tremendous need for security at United States borders. It ensures that individuals at our borders maintain some level of personal and digital dignity. Any lesser standard would subject every international traveler to "[what is] essentially a computer strip search."[192]

---

[192] *Cotterman*, 709 F.3d at 966.