Electronic Searches on the Physical Frontier

Prepared for:
John T. Morton, Director, Immigrations and Customs Enforcement
Thomas S. Winkowski, Acting Commissioner, Customs and Border Patrol

Authors:
Liz Fong-Jones <lizfong@mit.edu>
Austin Duffield <duffield@mit.edu>
Steven Allen <steb@mit.edu>

6.805, Fall 2013

Table of Contents

Executive Summary

We present a set of policy recommendations for the screening of electronic devices at border crossings that is less invasive than current policy, but maintains existing levels of protection of the United States's physical borders and security given the threat model of porous internet borders. We propose that customs agents should be allowed to perform cursory searches of electronic devices without suspicion, forensically search electronic devices physically present before them for inspection at a checkpoint with reasonable suspicion, but should not be allowed to retain devices or data unless they discover a customs or immigration violation. Furthermore, US citizens should be allowed to delete their data rather than submit to a search. This represents a change from the current policy that permits indefinite obligatory seizure of devices and forensic examination offsite without reasonable suspicion. These changes are prudent both because they allow for limited resources to be more efficiently spent and because they are more likely to survive legal scrutiny in the current judicial climate.

Introduction

The United States has maintained vigilant inspection of travelers and goods crossing its borders for hundreds of years in order to enforce its immigration and customs policies. As a matter of fact, the border search exception dates back to the first customs statute (Act of July 31, 1789, c. 5, 1 Stat. 29, Section 24) enacted before the Bill of Rights (*United States v. Ramsey*, p. 431 U. S. 616). Representatives of the customs and immigration enforcement services perform searches without obtaining warrants for each individual search and regardless of the existence of particularized suspicion towards each searched individual.

Ordinarily, performing searches in this manner would contravene the Fourth Amendment prohibiting unreasonable searches and seizures. Instead, a "border search exception" has historically applied to individuals and their possessions at physical checkpoints along the border and at ports, and freight and postal mail shipments at ports; it allows officials to perform warrantless searches in order to determine whether a traveler is behaving consistently with his or her visa, and whether he or she is carrying contraband.

Two elements are required in order to permit warrantless border searches

-- first, statutory authority, and second survival of constitutional scrutiny. The statutory authority for border searches arises from 8 U.S.C. § 1357(c), which states,

> Any officer or employee of the Service authorized and designated under regulations prescribed by the Attorney General, whether individually or as one of a class, shall have power to conduct a search, without warrant, of the person, and of the personal effects in the possession of any person seeking admission to the United States, concerning whom such officer or employee may have reasonable cause to suspect that grounds exist for denial of admission to the United States under this chapter which would be disclosed by such search.

As for the constitutionality argument, the border search exception (BSE) is not explicitly mentioned in the Constitution. Instead, it is a legal doctrine established by judicial precedent that permits warrantless searches that would otherwise be impermissible under the Fourth Amendment. Under the doctrine, a traveler's attempt to cross a border constitutes in and of itself reasonable grounds for a search even without a warrant, and therefore the prohibition against unreasonable searches does not apply. The Supreme Court re-affirmed in 1977 that "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border" [1], noted that the same Congress that proposed the Bill of Rights also granted Customs the right to perform border searches without a warrant, and further cited historical Supreme Court precedent from *Carroll v. United States* that "national self-protection reasonably [requires] one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in" (1932) [2]. However, the BSE does not immunize officials from claims based upon the First Amendment or Fifth Amendment and thus searches must not be targeted based on First Amendment protected speech or behavior, and may not force an individual to incriminate himself or herself.

The current agencies performing border searches are Customs and Border Patrol (CBP) and Immigration and Customs Enforcement (ICE), both branches of the Department of Homeland Security in the executive branch of the United States government. Accordingly, their policies and procedures are subject to modification by executive order. Other branches of government influence the search procedures through legislation and judicial decisions. Congress has

historically supported expansion of warrantless border searches [3], but the courts have recently begun reining in more liberal extensions of the border search exception [4].

The advent of digital technology has shifted the privacy landscape, resulting in a need to further clarify how the border search exception should apply to electronic devices. At present, CBP and ICE policy [5] does not give electronic devices containing data different treatment than non-digital items, and reserves the right to examine them as they would a file full of documents. They may detain physical devices or make copies for off-site analysis and return devices. Their retention policies specify that data is to ultimately be deleted if no evidence of wrongdoing is found, but may be retained for up to thirty days initially with indefinite extensions [6] and have forensic examination performed upon it. Currently, if, in the course of a warrantless search for customs and immigration violations under the border search exception, probable cause is found for a non-immigration and non-customs matter, the material may be handed over to other authorities and the data retained for further investigation and prosecution.

New Challenges of Electronic Border Searches

Travelers use digital luggage in fundamentally different ways than they use physical luggage; thus, border searches of electronic data requires modifying the legal scheme originally established for physical luggage to account for the differing privacy expectations. The analogy between a hard disk and a file folder of papers or a suitcase full of belongings breaks down in multiple ways. Since storage space is relatively unlimited and cleanup is difficult, travelers often carry their entire digital lives with them rather than only the few specific things pertinent to their travel plans. The intent of examinations of personal effects for immigration purposes is to ascertain whether someone's possessions match their stated purpose of visit, but this type of examination becomes moot with an indiscriminate trawl through *all* of someone's digital files, which will not reflect a deliberate choice pertinent to an immigration investigation of which files to bring with them on their trip. Furthermore, conducting a diligent search of someone's entire digital life within the span of a customs interview requires an inordinate amount of effort, and is more intrusive than an ordinary search of physical possessions.

Intrusiveness and Purpose of Forensic Examinations

The set of documents carried with an individual on an electronic device tend to be more private in nature than physical documents because individuals advertently or inadvertently leave very private information on their devices in the course of using them and do not take the time to meticulously clean the contents of their computers prior to travel. In *United States v. Cotterman* [18], the Ninth Circuit ruled that seizure of a device for customs purposes and its subsequent forensic examination constituted a "particularly offensive" invasive search similar to a strip search or cavity search in levels of intrusiveness upon an individual's privacy, and required reasonable suspicion rather than the simple warrantless, suspicionless routine searches typically performed. In particular, the Ninth Circuit cited the types of data typically carried -- "financial records, confidential business documents, medical records and private emails" [18], and was concerned that such information might constitute thoughts and ideas subject to freedom of conscience from government intrusion. Furthermore, it found that users who make an effort to delete data may not be aware that superficially deleted files may still be recoverable by forensic examination, or that internet browsing histories are automatically saved to storage.

In the case, Cotterman's person and contents of his vehicle were searched upon his return to the United States from Mexico by car due to Cotterman's presence on a watchlist of individuals suspected of trafficking in child pornography. During the search of Cotterman's laptops and cameras by ICE agents at the checkpoint, no evidence was found immediately suggesting criminal activity, aside from the presence of several encrypted files; nevertheless, the devices were seized and taken offsite to an ICE office for a more detailed forensic examination. Cotterman's attorneys moved to suppress the evidence under the theory that the transportation of the seized devices for the search created an extended border search requiring reasonable suspicion, which the agents could not have found based on the circumstances at the border. The Ninth Circuit rejected that interpretation, and instead stated that the search was an ordinary border search because it began at the border regardless of how far the devices were subsequently transported; regardless, it ruled that forensic examination of digital devices did constitute a "particularly offensive" search requiring reasonable suspicion. However, it found that reasonable suspicion could have been shown by the officers, and reversed the District Court's suppression of the evidence. At issue in the Supreme Court appeal is whether the Ninth Circuit made procedural errors in making a fact-finding that reasonable suspicion was present and considering an issue abandoned by the prosecution, and furthermore whether

the Ninth Circuit erred in deciding that the indefinite detention of and transportation of Cotterman's possessions was permissible without suspicion.

Beyond use of border searches for customs or immigration purposes, law enforcement has been using the border search exception to carry out ordinary law enforcement rather than restricting its use to the highly specific purpose of customs and immigration. Individuals such as Jacob Appelbaum and David Miranda have been detained during customs and immigration processing and have had their digital devices forensically imaged with no apparent connection to customs and immigration purposes. Instead, the search appears to be targeted instead at finding evidence of prior disclosure of damaging government secrets.

Plain View Exception

According to the "in plain view" doctrine established by the U.S. Supreme Court in *Horton v. California,* 496 U.S. 128 (1990) [19]:

> The Fourth Amendment does not prohibit the warrantless seizure of evidence in plain view even though the discovery of the evidence was not inadvertent.

What is "in plain view" digitally may be very different from what is "in plain view" physically under the plain view doctrine. Circuit courts are in disagreement on the issue -- the Fourth Circuit ruled in *United States v. Williams*, No. 09-3174 (2010) that digital devices seized for one purpose could be freely examined in their entirety [21] but the Second Circuit ruled in *United States v. Galpin*, 11-4808 (2nd Cir. Jun. 25, 2013), that it was impermissible to perform a search of a digital device under one premise but in actuality fail to minimize the portion of the device examined to the pertinent details [20][7].

In *United States v. Williams*, Curtis Robert Williams was convicted of possession of unregistered firearms and child pornography. For the sake of brevity, we will not summarize any parts of this case related to the firearms and instead focus on the search of his digital devices. Williams was initially suspected of sending threatening emails concerning children who attended his church. The government therefore obtained a warrant authorizing the search and seizure of [21]:

> Any and all computer systems and digital storage media, videotapes, videotape recorders, documents, photographs, and Instrumentalities

> indicat[ive] of the offense of § 18.2-152.7:1 Harassment by Computer and § 18.2-60 Threats of death or bodily injury to a person or member of his family; threats to commit serious bodily harm to persons on school property, Code of Virginia (as amended).

During the search of a DVD for evidence of the threats mentioned in the warrant, the FBI agent performing the search discovered images whose thumbnails revealed some of them to be child pornography.

In his appeal, No. 10-6854 (4th Cir. Oct. 22, 2010), Williams argued that (a) the search for child pornography did not fall within the scope of the warrant and that (b) the officers intended to find evidence of child pornography and that the "in plain view" doctrine did not apply because the discovery was not inadvertent, a requirement set in place by the 10th circuit court in *United States v. Carey*, 172 F.3d at 1273. However, the court found that (a) the child pornography fell within the scope of the warrant because it was an "Instrumentalit[y]" and that (b) regardless of (a), the 10th circuit's ruling in *Carey* was overruled by *Horton v. California* where the Supreme Court ruled that [19]:

> The fact that an officer is interested in an [unauthorized] item of evidence and fully expects to find it in the course of a search should not invalidate its seizure if the search is confined in area and duration by the terms of a warrant or a valid exception to the warrant requirement.

Therefore, according to Fourth Circuit search intentions are irrelevant.

However, the Second Circuit found differently. In *United States v. Galpin* the United States charged Galpin with position of child pornography, production of child pornography, and committing a felony offense involving a minor while being required to register as a sex offender. In support of their case, the Government brought forth evidence derived from a broad search of Galpin's computers and digital recording equipment. Galpin sought to exclude this evidence arguing that the warrant was overbroad. The United States Court of Appeals for the Second Circuit found that (a) the warrant was overbroad, (b) the lower court did not sufficiently demonstrate the warrants severability, (c) the lower court must review its application of the "in plain view" doctrine given the narrowed warrant, and (d) the lower court should review the government's argument that the evidence was found "in good faith."

In regards to the application of the "in plain view doctrine" the court stated that that (p. 23):

> However, the district court's review of the plain view issue should take into account the degree, if any, to which digital search protocols target information outside the scope of the valid portion of the warrant. To the extent such search methods are used, the plain view exception is not available.

In other words, if a search targets files outside of the scope of the warrant, the in plain view exception may not be used.

Potential for Supreme Court intervention

Because of this disagreement between circuit courts over issues of the Border Search Exception and the Plain View Doctrine when digital devices are seized as evidence, the Supreme Court very well could take up the issue in its next term in *Cotterman* [18].

The Border Search Exception Applied To Digital Devices

We begin our analysis by extending existing analysis of the BSE and applying it to digital device searches. The legality of warrantless border searches of physical items has been well-studied over the past several decades and courts have relatively clearly established the legal limits of such searches. However, very few sources deal with searches of electronic devices, and even fewer studies do so in an unbiased manner. Most are either authored by the government and heavily favor broad search powers [8] or are authored by groups such as the ACLU [9] and EFF and offer insightful but uncompromising criticism without practical legal proposals. In this section, we expand on an analysis written by Jon Adams in 2005 which provides a comprehensive and pragmatic overview of the applications and limits of the border search exception in the context of non-digital luggage.

In 2005, Jon Adams, former assistant attorney general of New Mexico, released a comprehensive legal analysis [11] of non-digital border searches. In his analysis, he notes that the border search exception applies to both inbound and outbound travelers, non-routine searches require reasonable suspicion, and that seizures of luggage are equivalent to seizures of persons and must be time limited.

Outbound And Inbound Searches

In arguing that the border search exception applies equally to outbound as it does to inbound travelers, Adams (2005) cites *United States v. Berisha* 925 F.2d 791 (5th Cir. 1991) noting that customs agents can search for undeclared "monetary instruments" valued in excess of $10,000. Therefore, the applicability of this argument to the search of digital devices hinges on whether or not a customs agent could have reason to believe that monetary instruments in violation of 31 U.S.C § 5316 might exist on a digital device.

In *United States v. Berisha* 925 F.2d 791 (5th Cir. 1991), the US government alleged that Berisha attempted to carry $17,000 across an international border without making a declaration pursuant to 31 U.S.C § 5316. Berisha only declared $8,000 to an inspector, indicating a bulge in one of his front pockets. Noticing a bulge in the other front pocket, the inspector searched him and discovered $9,000 more. In an attempt to suppress this evidence, Berisha argued that the search violated the fourth amendment. The court ruled that the search was legal by statute citing 31 U.S.C. § 5317(b) which grants customs agents the power to search, without a warrant, for "monetary instruments" in violation of 31 U.S.C § 5316 (p.355), in other words, cash or cash equivalents in excess of $10,000. The court argued that the search was reasonable, and therefore constitutional, because, as stated in *United States v. Ramsey*, "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border...." (431 U.S. 606, 616, 97 S.Ct. 1972, 1978, 52 L.Ed.2d 617 (1977)).

Therefore, as, according to the ICE Homeland Security Investigations, “[t]he language [of the statute] requires something that can be passed from one individual to another in order to be presented to a third party for execution/payment." As data can only be copied, not passed, it would not be governed by this statute and this statute would not allow the government to search the digital effects of leaving persons. Interestingly, and incorrectly, the government echos Adams reasoning when claiming the right to search the digital effects of departing persons [6].

However, the government does, in fact, have the right to search departing digital devices under the Arms Export Control Act (22 USC Chapter 39). The Arms

Export Control Act forbids the export of cryptographic software if, for example, the software is not correctly registered. As noted by Cunningham, “some courts have also found statutory authority for exit searches in 22 U.S.C. § 401, which authorizes the seizure of illegally exported war materials.” [12] This, in conjunction with the Arms Export Control Act, gives the government the statutory right to search digital devices leaving the country for unregistered or improperly registered cryptographic software.

Non-Routine Searches

Adams (2005) also notes that non-routine searches require reasonable suspicion, a requirement that extends to forensic examination of digital devices. According to Adams, "Ordinarily, a stop or search more extensive than a routine search requires reasonable suspicion" (p. 356). In contrast, according to a recent Ninth Circuit appeal, *United States v. Cotterman*, a customs agent needs reasonable suspicion to forensically examine digital devices but needs no suspicion to perform a cursory examination. This means that, according to the Ninth Circuit Court Of Appeals, forensic examination of digital devices falls under the non-routine header and requires reasonable suspicion.

Detention of Luggage and Person

In Adams’ analysis, he notes that, based on *United States v. Thirty-seven Photographs*, 402 U.S. 363 (1971), the government must begin forfeiture proceedings within 14 days of the seizure (p. 271). In *United States v. Thirty-Seven Photographs* 402 U.S. 363 (1971), US customs agents had seized obscene photos from Luros on October 24th on his return to the united states. The united states brought forfeiture proceedings on November 6th. Luros argued both that (a) the government waited too long before bringing forfeiture proceedings and that (b) the government could not seize obscene material for private use under the 1st amendment. The U.S Supreme Court denied his claim because (a) the government brought forfeiture proceedings within 14 days of seizure could have completed district court proceedings within another 60 days and (b) because the first amendment does not protect obscene speech.

Here, the court ruled that, in the case of seizure of obscene materials at the border, "forfeiture proceedings be commenced within 14 days and completed within 60 days of their commencement" (p. 374):

> Given this record, it seems clear that no undue hardship will be imposed upon the Government and the lower federal courts by requiring that forfeiture proceedings be commenced within 14 days and completed within 60 days of their commencement; nor does a delay of as much as 74 days seem undue for importers engaged in the lengthy process of bringing goods into this country from abroad.

However, contrary to Adams' claim, the court does note that this restriction depends on the context and this ruling should not be over generalized (p. 374):

> Of course, we do not now decide that these are the only constitutionally permissible time limits. We note, furthermore, that constitutionally permissible limits may vary in different contexts; in other contexts, such as a claim by a state censor that a movie is obscene, the Constitution may impose different requirements with respect to the time between the making of the claim and the institution of judicial proceedings or between their commencement and completion than in the context of a claim of obscenity made by customs officials at the border. We decide none of these questions today.

While this decision does not set a specific time limit for general seizure proceedings, it indicates that such a time limit must be set.

However, according to the CBP, they may detain electronic devices [12], before seizing them, for an infinitely extendible period of time. Based on the aforementioned ruling, this detention period would likely be found unconstitutional as the ruling in *United States v. Thirty-seven Photographs* clearly indicated that the constitutionality of the statute in question (In *United States v. Thirty-seven Photographs*) hinged on its time limit. In essence, the CBP claims that it has the right to indefinitely detain a traveler's belongings.

Extreme Proposal Options

Individuals bear a responsibility to not import illicit content regardless of whether it is a standalone physical object such as a bootleg DVD or resides as electronic data upon an individual's device as a ripped movie. However, with the exceptions of nations such as China which practice systematic filtering and censorship, the internet crosses international borders without overt customs checks. Therefore, merely searching the subset of a person's electronic data that

happens to be physically with them critically omits the fact that they could import contraband data into the United States via other means. Given the intrusiveness of the search and the marginal effectiveness of the search, the United States must consider, as this paper does, whether the disparity in strictness should be addressed by tightening controls on internet traffic or by relaxing the use of border searches upon electronic devices.

In order to understand the complexities of this issue and gain some insight into how a potential solution can be analyzed, we look at the two most extreme possible policies. A restrictive approach of searching everything and a permissive approach of searching nothing are both obvious attempts at clarifying border search policy. Both strategies have severe legal and logistical flaws, but they reveal important factors that must be considered when discussing recommendations in the next section.

Restrictive

On the most restrictive end of the spectrum, the United States could inspect all data that enters or leaves the country. In this approach, all physical storage media would be searchable at border crossings. The policy is indistinguishable from the status quo legislation, but far more extreme in practice, involving the search of a tremendous quantity of information. A large array of software tools and supporting maintenance and enforcement infrastructure would have to be developed to automate the process. Current device search practices are quite narrowly targeted, affecting approximately 5,000 individuals in 2011 and 2012 [14], but under a "total search" policy, the number of device searches would approach the number of luggage searches, affecting a much larger number of people passing through customs.

While such a strict observation of data in transit is very attractive to security agencies, as it provides greater control and oversight over information crossing US borders, two immediate loopholes are evident with a policy like this. First, the internet crosses borders without customs checks, and can thus be used to shuttle illegal data across borders. Second, encryption would effectively prevent meaningful information being obtained from device data within a reasonable period of time or a reasonable budget.

It is easy to come up with solutions to these loopholes consistent with the

conservative policy approach. To prevent illicit material from crossing borders via the internet, CBP and ICE would be given the authority to inspect international internet traffic in addition to physical media. To prevent encrypted material from crossing borders, travelers would be required to decrypt all data on physical media at the border, allowing analysis software to access this content.

With this complete policy option, several logistical issues are evident. First, encrypted content could still travel over the internet. There is no obvious solution to this, as requiring its decryption would be infeasible. Second, the quantity and variety of electronic devices crossing borders would present a daunting challenge to software attempting to analyze these devices. It would be infeasible to remove storage media from all devices, as this is both time-consuming and invasive, so analysis software would have to be capable of interacting with the wealth of operating systems running on consumer devices, which is far from trivial.

Legal issues are also evident. Though legislation and court opinions have been generally permissive in the flexibility it affords to border agents through the border search exception, the thorough forensic analysis of devices is unlikely to be considered justified. Additionally, seizure of data for later remote analysis would require a separate justification. It is unclear whether or not the border search exception would permit this, but a challenge on Fourth Amendment grounds would certainly have strong backing.

Permissive

On the permissive end of the policy spectrum, the US could take a "hands-off" approach and ignore data in electronic storage media. Such a policy would require codifying several privacy protections and a significant shift in current policy trends and thinking. Practices would actually change little though, as border searches are uncommon in the status quo.

This policy obviously fails to address the customs problem though, permitting illicit data to cross borders unchecked. It also falls far short of the flexibility currently afforded border agents under the border search exception, so it could add burdensome limitations. Because much of the circumstances under which a device is chosen to be searched have not been disclosed by CBP and ICE, it is possible that a liberal approach would put in place a restriction that causes unanticipated harm, hampering an investigation.

What We Gain from Extreme Options

Obviously, the extreme restrictive and extreme permissive policy approaches would never be seriously considered in practice, but they provide two key considerations to take into account when approaching our recommendations.

First, we must take into account the feasibility of a policy in addition to its legal implications. A primary reasoning for making these recommendations is to take the present state of technology into account - what is possible should certainly inform what is recommended. Additionally, it is much easier to determine the feasibility of an approach than its legality. Whenever it is possible to substitute a technological argument for a legal one, this should be done. Among other things, this approach will make discussing encryption integral to our policy analysis.

Second, as discussed with the liberal policy approach, we must remember that not all information is known about border device searches. While a great deal of information on the circumstances and consequences of a search is available or easily inferred, it is important, when possible and sensical, to avoid removing key flexibility available to border officials.

Recommendations

Based on analysis of the two extreme solutions and the prior art discussed earlier, we recommend the following policy:

Customs agents should be allowed to search electronic devices physically before them, but should not retain devices or data for forensic investigation without reasonable suspicion. US citizens should have the option to delete the data from electronic devices rather than submit to a search.

This particular set of requirements stems from the federal court's past decisions that define the scope of the Border Search Exception and takes into consideration the effectiveness and practicality of a modern border search system. Next, we will discuss each component of this recommendation in detail, looking at where each derives from and what its implementation would be.

Physically Before Them

This component of our recommendation states that the entirety of a device search must take place at the border, in the presence of the owner and a border official. This seeks to reform the practice (as in *Cotterman* [18]) of confiscating electronic devices, shipping them to a forensics lab, and holding them there for months of intensive analysis. We argue that this practice is intrusive, and therefore unconstitutional under the Fourth Amendment, despite the Border Search Exception, because of the intensive and broad-based search method employed. We recommend that the search take place at the border and in the presence of the subject, as this is the most straightforward and transparent way to constrain a device search to a reasonable, narrowly-tailored exercise. Note that this recommendation applies to searches that do not meet the reasonable suspicion standard, but are simply routine as part of customs practices.

An important distinction that courts have made [14] is that between *routine* and *non-routine* searches. Routine searches are those that are carried out very commonly and do not require any justification under the Border Search Exception. Non-routine searches go beyond what is generally required to perform customs and thus require some justification. Though they are included under the Exception, non-routine searches have been held, in *United States v. Montoya de Hernandez* [15], to require meeting the reasonable suspicion standard.

There is no established test to determine whether or not a search is routine - this distinction turns on the level of intrusiveness of a given search procedure. The opinion in *United States v. Braks* [16] discusses six factors that contribute to the intrusiveness of a border search, most of which are irrelevant to electronic devices (things like disrobing, physical contact, etc do not generally apply), but two of which are relevant. One factor is the manner in which a search is conducted and another is the degree to which the subject has a reasonable expectation of privacy. We argue that performing a device search at the border in the physical presence of the owner is the least invasive way to conduct the necessary duties of customs and avoids intruding significantly on the owner's expectation of privacy.

The Ninth Circuit, in *United States v. Arnold,* [17] held that electronic devices are treated under law as "closed containers," meaning the same as suitcases or purses. The search of these devices epitomizes a "routine" search, and

as such we can use the manner in which these devices are searched as a model. At a border security checkpoint, these containers are sent through an x-ray machine. If anything unusual is displayed by the x-ray, then the container is quickly sifted through by hand, in the presence of the owner. Three things about this process are key: it is minimal, it is fast, and it takes place in the presence of the owner. The recommendation for a routine device search is consistent with all three of these guiding principles from a closed container search.

That the search occurs locally, carried out by an officer on site, is not necessary for the manner of the search to be non-intrusive. This is merely a procedural recommendation. It would certainly be possible, if the infrastructure were to exist, for a remote agent to perform a device search non-intrusively, "routinely." A routine search should be sufficiently minimal that the expertise of a remote party should not be necessary, but a requirement for such is not part of our recommendation. Our recommendation does, however, require that the device remain with the owner. A seizure of the device would be obviously be non-routine, as discussed in a later section on retaining devices and data.

Reasonable Suspicion

There are occasions in which a non-routine search, meaning any search that does not follow the method described above, must occur. Our recommendation is that a non-routine search occur when the reasonable suspicion standard is met.

The U.S. Supreme Court defined this standard in *Terry v. Ohio*, a case that dealt with police stopping and frisking a suspect to ensure that he or she was unarmed. Justice Warren's majority opinion in that case specifies that "specific and articulable facts", "taken together with rational inferences from those facts," must be presented to justify an action under "reasonable suspicion." The Terry situation is similar in spirit to a search performed for national security reasons, as both serve to protect against immediate threats to public safety during an investigation.

United States v. Montoya de Hernandez held that "'reasonable suspicion' effects a needed balance between private and public interests when law enforcement officials must make a limited intrusion on less than probable cause."[15] The majority opinion in that case discusses border-specific language

used by other courts to describe a similar standard, such as "clear indication" (*United States v. Ramsey*), but decides that such standards are not sufficiently well defined and would make it difficult for courts and border officials to make effective decisions. It further concludes that reasonable suspicion is functionally ideal for the situations that arise in border situations.

Retain Devices or Data

Treating a non-routine search of electronic devices under the auspices of national security with the same reservations as a Terry pat-down, we gain some further insight into procedures that must be followed to uphold the fourth amendment protection against unlawful search and seizure. Specifically, we can conclude that a routine search does not involve the seizure of devices or data, while a non-routine search may.

Searching an electronic device, whether routine or not, must be quick and minimal. Either type of search should employ the least means to ascertain that an individual does not carry contraband or present a threat to national security. During a pat-down, a police officer performs a "frisk," which is designed to use the least possible means in order to ascertain that a situation is safe. Similarly, a border search of an electronic device must be carried out in a reasonably short timeframe, and in a minimally-invasive manner.

In *United States v. Montoya de Hernandez*, the Supreme Court makes it explicit that a significant period of time can be justified under reasonable suspicion as long as it is "the period of time necessary to either verify or dispel the suspicion"[16], but no more time than this is justified. In the same case, the court ruled that a certain level of invasiveness was also justified under reasonable suspicion at the border, as long as this level is the minimum necessary to ensure border protection.

United States v. Cotterman specifies the forensic examination as the capability provided to border agents once this reasonable suspicion is established. [18] Due to the "comprehensive and intrusive nature" of forensic examination, reasonable suspicion must be a prerequisite. This sort of forensic examination includes three highly-invasive practices: seizure of devices, copying and storing data. Any of these would be considered non-routine under our recommendations, which treat the seizure of data and the seizure of data as equivalent.

This brings us to the distinction between routine and non-routine searches as applied to the Terry Stop analogy. Just as a police officer cannot reach into a suspect's pockets during a Terry Stop until reasonably suspecting that the pockets contain a weapon, a border agent cannot deeply inspect (forensically examine) an electronic device until being reasonably suspicious that it contains illicit information. This forensic investigation is a non-routine search, and can only be legally pursued if some suspicious information is found during a routine search. It is likely that a forensic examination of an electronic device would require specialized skills and equipment, and that the least means available to search it require sending the relevant data to a lab that has these skills and equipment available. This practice, as ruled in *Cotterman*, is the activity must offensive and most vulnerable to constitutional challenge, and thus the most important to restrict.

Optional Search For United States Citizens

Furthermore, we recommend that US citizens be given the option to discard their data rather than submit to a search. Unlike physical objects, digital devices often store vast quantities of sensitive data of which the bearer is often unaware. While a reasonable person would likely know the physical contents of his or her luggage, he or she would likely not know the contents of every file on his or her digital devices. Digital border searches are intended to both prevent illegal data from entering the country and to discover people entering the country in violation of their visa, not to discover evidence of a crime. According to 8 USC § 1357,

> Any officer or employee of the Service authorized and designated under regulations prescribed by the Attorney General, whether individually or as one of a class, shall have power to conduct a search, without warrant, of the person, and of the personal effects in the possession of any person seeking admission to the United States, concerning whom such officer or employee may have reasonable cause to suspect that **grounds exist for denial of admission** to the United States under this chapter which would be disclosed by such search.

As US citizens cannot, by definition, be in violation of a visa. Therefore, allowing US citizens to delete data instead of submitting to a search realizes this goal while

maintaining the citizen's privacy.

Arguments Against And Rebuttals

On-site searches are an unacceptable burden

One might argue that requiring that digital searches, even routine ones, be performed on-site puts too much of a burden on US Customs And Border Patrol due to a shortage of qualified experts. However, as (a) US CBP presently carries out approximately 5000 device searches per year [14] and (b) experts do not necessarily need to be physically present to perform a search, US CBP needs only to hire enough experts to carry out an average of approximately 14 device inspections per day. While the expert would operate remotely, the routine search would still effectively take place in front of the person whose device is being searched. Therefore, such a requirement can be met without excessively burdening the CBP.

Furthermore, one might argue that digital searches are time consuming and therefore should not be performed in front of the person whose computer is being searched in order to prevent unnecessary detention. However, as Adam (2005) noted [10] in his analysis, forcing someone to choose between leaving his or her luggage behind or staying with detained luggage constitutes detention of the affected person. Additionally, an expedient immediate search is actually less of a burden since it ensures that a traveler can be promptly sent on their way with their belongings if the search turns up no evidence of wrongdoing.

Optional digital searches will prevent customs agents from carrying out their mandate

One might also argue that allowing US citizens to delete their data instead of submitting to a search would be equivalent to allowing destruction of evidence. While the data, in fact, contain contraband, the contraband would still effectively be kept out of the country in keeping with the spirit of the border search exception. This solution is in accord with the dissent in *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985).

In United States v. Montoya de Hernandez, 473 U.S. 531 (1985), customs officials detained Hernandez suspecting her of smuggling drugs in swallowed

balloons. Customs agents offered her the option of returning home or submitting to an invasive search. While she opted to return home, she was unable to do so before the customs officials obtained a search warrant based on her suspicious refusal to eat, drink, or use the toilet. She was found to have been smuggling cocaine, arrested, and convicted. She then unsuccessfully attempted to reverse the conviction on the grounds that the search violated her fourth amendment rights.

However, in their dissent, Justice Brennan and Justice Marshall argue that (473 U.S. 531, pp. 563-564):

> [T]he Government in carrying out such immigration and customs functions does not simply have the two stark alternatives of either forcing [473 U.S. 531, 564] a traveler to submit to such procedures or allowing him to "pass . . . into the interior." Ante, at 544. There is a third alternative: to instruct the traveler who refuses to submit to burdensome but reasonable conditions of entry that he is free to turn around and leave the country. In fact, I believe that the "reasonableness" of any burdensome requirement for entry is necessarily conditioned on the potential entrant's freedom to leave the country if he objects to that requirement. Surely the Government's manifest interest in preventing potentially excludable individuals carrying potential contraband from crossing our borders is fully vindicated if those individuals voluntarily decided not to cross the borders.
>
> This does not, of course, mean that such individuals are not fully subject to the criminal laws while on American soil. If there is probable cause to believe they have violated the law, they may be arrested just like any other person within our borders. And if there is "reasonable suspicion" to believe they may be engaged in such violations, they may briefly be detained pursuant to Terry for further investigation, subject to the same limitations and conditions governing Terry stops anywhere else in the country. 36 But if such Terry suspicion does not promptly ripen into probable cause, such travelers must be given a meaningful choice: either agree to further detention as a condition of eventual entry, or leave the country.

Basically, absent probable cause, a person being subjected to an invasive search should be given the option to go home because going home effectively excludes any contraband they might be carrying. However, in this case, as the potential contraband is separate from the traveler, the potential contraband may simply be rejected alone and the traveler allowed to enter the country.

One might also argue that this proposal eliminates a deterrent against the import of contraband. That is, beyond simply denying the import of contraband, digital searches function to deter any attempts to import such contraband. As readily available alternative means of data transfer exist (the internet), such a deterrent is wholly ineffective. That is, anyone deterred from carrying contraband into the United States in a digital device would simply upload the content to his or her favorite online data storage service. Therefore, the search of digital devices does not serve as an effective deterrent.

Authority to Modify Border Search Procedures

This report makes practical policy proposals to better uphold the spirit of the border search exception and maintain the continued constitutionality of electronic device searches at borders. The statutory authority of Immigration and Customs Enforcement and Customs and Border Patrol is permissive rather than prescriptive; thus, CBP and ICE are not mandated by law to perform the specific kinds of particularly invasive searches at issue, nor to conduct them in any specific manner. CBP and ICE can make changes to policies and procedures that reduce the scope of the searches they perform, and do not require further intervention from Congress or from the judiciary branch to act. We believe, therefore that the director of ICE and commissioner of CBP have adequate authority to implement our recommendations for better adherence to the spirit of the border search exception when it comes to treatment of electronic device searches conducted by their respective agencies.

Conclusion

Technological and social changes have pushed existing border search jurisprudence beyond its previous analogies and legal reasoning. Warrantless examination still ultimately requires compliance with the Fourth Amendment prohibition on unreasonable searches and seizures. The waiver of a warrant depends on the existence of reasonableness implied by the United States Government's need to protect its borders. Unless the search scheme is changed, the Supreme Court may wind up striking down the existing warrantless electronic border search scheme. Therefore, it behooves CBP and ICE to act early and proactively craft policies that will survive judicial review rather than having

evidence struck down, convictions overturned, and procedures thrown into chaos.

Therefore, we recommend that while customs agents should be allowed to search electronic devices, they should conduct their searches in a manner that minimizes intrusiveness. To achieve this, we propose that customs agents not retain devices or data for forensic examination without reasonable suspicion. Furthermore, we recommend that US citizens be allowed to delete their data rather than submit to a search. These proposals uphold the intention of the BSE by ensuring that the CBP can effectively exclude contraband and persons entering the United States in violation of their visa while reducing invasiveness.

Bibliography

[1] *United States v. Ramsey*. 431 U.S. 606, 97 S. Ct. 1972, 52 L. Ed. 2d 617 (1977)

[2] *Carroll v. United States*. 267 U.S. 132

[3] United States. Cong. House Of Representatives. 111th Congress, 2d Session. H.R. 4941, Anti-Cash Smuggling Act of 2010, introduced in the U.S. House Of Representatives; 25 March 2010, 111 Cong., 2d sess., Congressional Bills, GPO Access, Web. 11 December 2013 <http://www.gpo.gov/fdsys/pkg/BILLS-111hr4941ih/pdf/BILLS-111hr4941ih.pdf>

[4] *Almeida-Sanchez v. United States* , 413 U.S. 266, 272-76 (1973)

[5] U.S. Customs and Border Protection. *Policy Regarding Border Search of Information* (2008)

[6] Kim, Yule, "Border Searches of Laptop Computers and Other Electronic Storage Devices." 16 November 2009. RL34404. *Federation of American Scientists CRS Reports.* Web. 11 December 2013.

[7] Kerr, Orin. "Second Circuit Suggests That the Plain View Exception Should Be Applied More Narrowly to Digital Searches." Web log post. *The Volokh Conspiracy*. N.p., 25 June 2013. Web. 20 Dec. 2013.

[8] Schlanger, Margo. "Border Searches of Electronic Devices." *Civil Rights/Civil Liberties Impact Assessment*. U.S. Department of Homeland Security, 29 December 2011. Web. 22 October 2013

[9] "Border Search | American Civil Liberties Union." Web log category. *Blog of Rights*. American Civil Liberties Union. Web. 22 Oct. 2013. <https://www.aclu.org/blog/tag/border-search>

[10] Jon, Adams. "Rights at United States Borders." BYU Journal Of Public Law 19.2 (2005): 353-71. Web.

[11] Cunningham, Larry. "Border Search Exception as Applied to Exit and Export

Searches: A Global Conceptualization, The." *QLR* 26 (2007): 1.
[12] "Border Search of Electronic Devices Containing Information", CBP Directive No. 3340-049. CBP, 20 August 2009. Web. 22 Oct. 2013.
[13] Hauss, Brian. "Documents Shed Light on Border Laptop Searches." Web log post. *Free Future*. American Civil Liberties Union, 09 Sept. 2013. Web. 12 Dec. 2013.
[14] Kim, Yule, "Protecting the U.S. Perimeter: Border Searches Under the Fourth Amendment." 29 June 2009. RL31826. *Federation of American Scientists CRS Reports.* Web. 11 December 2013.
[15] *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985)
[16] *United States v. Georgette BRAKS*, 842 F.2d 509 (1998)
[17] *United States v. Arnold*, 533 F.3d 1003, 1009 (9th Cir. 2008)
[18] *United States v. Cotterman,* No. 09-10139 (9th Cir. en banc. 2013)
[19] *Horton v. California*, 496 U.S. 128 (1990)
[20] *United States v. Galpin*, 11-4808 (2nd Cir. Jun. 25, 2013)
[21] *United States v. Williams*, No. 09-3174 (2010)