Balancing Interests at the Border: Protecting Our Nation and Our Privacy in Border Searches of Electronic Devices

Carolyn James

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation

Available at: http://digitalcommons.law.scu.edu/chtlj/vol27/iss1/6
Balancing Interests at the Border: Protecting Our Nation and Our Privacy In Border Searches of Electronic Devices

Carolyn James†

Abstract

An analysis of the Department of Homeland Security's 2009 Directives on Border Searches of Electronic Media reveals the difficulty in striking a balance between protecting government interests in protecting the borders and preserving travelers' privacy interests. The 2009 Directives take some steps towards reaching this balance. They do not, however, adequately protect travelers' privacy interests, especially when taking into account the vast amount of personal information that electronic devices now carry. I make three suggestions to better strike this delicate balance: (1) Border officials should be required to have at least some reasonable suspicion before searching an electronic device; (2) Congress should require the DHS to conduct annual studies of their border searches, report their findings to Congress, and annually issue updated and concrete directives; and (3) Congress should require airlines to better inform travelers of the broad authority that border officials have in searching electronic devices.

I. INTRODUCTION

The August 2009 Department of Homeland Security (DHS) Directives on border searches of electronic devices and electronic media add additional guidelines to existing DHS policies;¹ however,

† Carolyn James is a third-year law student at Santa Clara University School of Law and serves as Senior Production Editor for the Santa Clara Computer and High Tech Law Journal. She also holds a B.S. in electrical engineering from Penn State University. She thanks Professor Allen Hammond and the CHTLJ editors for their valuable feedback on this article.

officials continue to wield vast discretion to search any electronic device at the border. Potential detection of terrorist activity and confiscation of contraband are the goals behind the broad power conferred upon border officials. While these policies are unquestionably important, they are countered by strong privacy interests. Laptops and other electronic media contain an immense amount of information that is highly personal to the device’s owner. With the ability to recover even deleted and encrypted files, customs officials have the keys to people’s lives at their fingertips when they conduct searches of electronic media.

Analysis of the 2009 DHS Directives, in context with the border search doctrine, reveals the current imbalance between the government’s interest in protecting the borders and travelers’ privacy interests. What is needed to rebalance these interests is: (1) a requirement that each border official have at least some reasonable suspicion before searching an electronic device at the border; (2) a requirement that the DHS conduct annual studies of their border searches, report the findings to Congress, and annually issue updated and more concrete directives; and (3) efforts to make travelers better aware of border officials’ broad authority to search electronic devices.

Electronic information does not need to cross the physical “border” while stored in an electronic device to be transferred across the border. Therefore, the rules regulating border searches of electronic media should require at least some suspicion because searches of electronic media within U.S. borders require a warrant. If at least some suspicion is required, border searches will be more efficient and travelers’ privacy interests will be better protected.

Moreover, to reach the delicate balance between homeland security concerns and privacy interests, Congress should pass

---


3. See United States v. Romm, 455 F.3d 990, 1006 (9th Cir. 2006); see 2009 ICE Directive, supra note 2, § 8.4; see 2009 CBP Directive, supra note 2, § 5.3.2.2.

legislation requiring the DHS to conduct an annual study of their searches and seizures. The report should include the types of searches conducted; the circumstances of the searches; the results of each search; and the race, gender, and national origin of travelers subject to the searches. The findings should be reported to Congress and, based on the study results, the DHS should be required to annually improve and clarify the policies governing border searches of electronic devices. The tailored policies and more frequent oversight would ensure border officials have appropriate discretion to support the Government’s interests and would provide more specific regulations to accommodate travelers’ privacy interests.

Finally, travelers should be better warned of the DHS’s broad authority to conduct searches of electronic devices when making plans to travel internationally. Congress should require airlines to give notice to travelers of the DHS’s authority during the ticket purchasing process before the ticket is officially purchased, on the airline website, and on the airline ticket itself. These are practical methods to inform travelers and will allow travelers to take actions to protect their privacy interests at the border.

II. BACKGROUND OF BORDER SEARCHES OF ELECTRONIC DEVICES

Under the Fourth Amendment, searches and seizures conducted by government agents must be reasonable and supported by probable cause. The Supreme Court has interpreted the Fourth Amendment to require a warrant for searches and seizures with some circumstantial exceptions. The Court has explained that law enforcement practices are “judged by ‘balancing its intrusion on the individual’s Fourth Amendment interests against its promotion of legitimate governmental interests.’” However, there is a “border search” exception that allows routine searches of persons and their belongings at the U.S. borders without the requirement of reasonable suspicion,

5. U.S. CONST. amend. IV (grants “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”).


7. See Mincey v. Arizona, 437 U.S. 385, 393-94 (1978) (“warrantless search must be ‘strictly circumscribed by the exigencies which justify its initiation.’” (quoting Terry v. Ohio, 392 U.S. 1, 25-26 (1968))).

probable cause, or a warrant.\footnote{United States v. Ramsey, 431 U.S. 606, 616 (1977) (stating "[t]hat 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, should, by now, require no extended demonstration.").} While non-routine border searches of a person require reasonable suspicion, these searches are limited to those that are "highly intrusive."\footnote{United States v. Flores-Montano, 541 U.S. 149, 149 (2004).} Only physically intrusive searches such as strip searches, body cavity searches, and x-ray searches of the human body have been found "highly intrusive."\footnote{United States v. Ramos-Saenz, 36 F.3d 59, 61 (9th Cir. 1994).}

The Ninth Circuit held that searches of electronic media, including laptops, are routine searches; thus, such devices are included in belongings that may be searched at the border without reasonable suspicion.\footnote{United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008) ("[W]e are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."); see also Romm, 455 F.3d at 1006 (holding "ICE's forensic analysis of Romm's laptop was permissible without probable cause or a warrant under the border search doctrine.").} Since international airports serve as functional borders,\footnote{Joelle Hoffman, Reasonable Suspicion Should Be Required at a Minimum for Customs Officials to Execute a Search of a Laptop at U.S. Borders: Why U.S. v. Arnold Got it Wrong, 36 W. ST. U. L. REV. 173, 182 (2009).} passengers who enter or leave the country\footnote{Nathan Alexander Sales, Run For the Border: Laptop Searches and the Fourth Amendment, 43 U. RICH. L. REV. 1091, 1099-100 (2009) (citing Patricia L. Bellia, The Memory Gap in Surveillance Law, 75 U. CHI. L. REV. 137, 144 (2008) "A modern-day 250-gigabyte hard drive is capable of storing the equivalent of 125 million printed pages of text.").} may have their laptops and other forms of electronic media searched without reasonable suspicion.\footnote{See Orin Kerr, Searches and Seizures in a Digital World, 119 HARV. L. REV. 531,}

A. Travelers' Privacy Interests Implicated by Searches of Electronic Media

Searches of electronic devices implicate important privacy and dignity interests.\footnote{E.g., United States v. Swarovski, 592 F.2d 131, 133 (2d Cir. 1979) (holding border search exception applies to items leaving as well as entering the country).} Searches of laptops and other forms of electronic media are different from searches of a person's wallet or briefcase because electronic media contains exponentially more information than wallets or briefcases,\footnote{Arnold, 533 F.3d at 1008.} and often contains information the owner does not know is stored on the device.\footnote{See Orin Kerr, Searches and Seizures in a Digital World, 119 HARV. L. REV. 531, 522 (2005). A modern-day 250-gigabyte hard drive is capable of storing the equivalent of 125 million printed pages of text.}
and other electronic devices can reveal as much or more information as a search of the person’s home. One law professor described the search of a laptop by a government agent as:

read[ing] your mind and everything you have thought over the last year. What a laptop records is as personal as a diary but much more extensive. It records every Web site you have searched. Every e-mail you have sent. It’s as if you’re crossing the border with your home in your suitcase.

Electronic devices carried internationally may contain personal pictures, contact information for all of the owner’s acquaintances, years of sent and received e-mails, saved files containing years of work, credit card information, passwords, and more.

Many individuals traveling internationally who enter, depart, or pass through the U.S. through international airports are unaware that their laptops and other electronic devices may be searched. Even if information is deleted or encrypted, the searches can recover the deleted information and can unencrypt encrypted information. Therefore, travelers who wish to carry electronic media with them into or out of U.S. borders are subject to the possibility of giving up personal information to the U.S. Government that they did not know was accessible from their electronic device.

B. The Government Has a “Paramount” Need to Protect U.S. Borders from the Entrance of Terrorists and Contraband

The significant privacy concerns of travelers must be balanced with the Government’s “paramount” need to protect the U.S. from the...
entry of terrorists and contraband into the country. The government also has a strong interest in searching outbound electronic devices to enforce export control laws protecting sensitive technologies and to prevent unwanted transmission of classified information.

Laptops and other electronic devices are unique in that they contain extraordinary storage capacity that can contain illegal materials. The government has a strong interest in preventing the distribution of child pornography and other "obscene" materials stored on laptops passing through the U.S. borders. The DHS describes border searches of electronic devices as "essential to enforcing the law at the United States Border" and as a crucial tool in detecting evidence relating to terrorism and other national security matters, narcotics and human smuggling, alien admissibility, contraband, and child pornography. The searches can also reveal information regarding violations of copyright, trademark, or export control laws. The DHS asserts that the "latest method" for smuggling merchandise contrary to the law is through the use of electronic materials.

The DHS's broad authority to search electronic devices at the border has facilitated detection of some terrorist activity and discovery of child pornography. For example, a laptop search at Minneapolis-St. Paul Airport in 2006 uncovered a laptop containing information on how to make improvised explosive weapons, weapons often used by terrorists in Afghanistan and Iraq, and videos using the weapons to kill soldiers and destroy vehicles. Numerous border searches of electronic devices have also uncovered child pornography and evidence of child exploitation. In June 2008, the Customs and Border Protection (CBP) bureau of the DHS released an article

26. Sales, supra note 17, at 1098.
29. Id.
31. Sales, supra note 17, at 1096 (citing Remarks of Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Security, at the Ctr. For Strategic and Int'l Studies (Dec. 19, 2006), http://www.dhs.gov/xnews/speeches/sp_1166557969765.shtm (last visited Feb. 27, 2009)).
32. See, e.g., Arnold, 533 F.3d 1003; Ickes, 393 F.3d 501.
declaring the importance of broad authority to conduct border searches of electronic devices and gave examples of illegal activity detected through the searches. These examples included three incidents of terrorist activity, one example of an intellectual property right violation, and one example of a search uncovering child pornography. Thus, the strong government interests in preventing terrorist activity and entrance of contraband information is facilitated through border searches of electronic devices.

While the DHS has not disclosed the specific number of suspicionless searches of electronic devices at the border, the number of searches that uncover terrorist information or other illegal activity, or the search methods used, an October 2008 statement by Jayson Ahern, Deputy Commissioner of the CBP, likely gives a fairly accurate estimate of the success rate of laptop searches. In October 2008, Ahern revealed that of the 169 laptops searched at the border in August 2008, only two were seized; a 1.4% success rate. Another ten laptops were detained for further analysis such as decryption or language translation. Furthermore, the two seized laptops were not seized for information stored within; one was outfitted to smuggle drugs and the other was contraband itself. These figures are likely representative of most border searches of electronic media, thus, only a very small number of searched devices reveal information that the DHS seeks to prevent from entering or exiting the country.

---

34. *Id.*
37. *Id.*
38. *Id.*
C. Previous Department of Homeland Security Policies on Border Searches of Electronic Devices

The Homeland Security Act of 2002 established the Department of Homeland Security and created the presidentially appointed position of Secretary as the head of the Department. The Act also created a Directorate of Border and Transportation Security headed by an Under Secretary for Border and Transportation Security. The United States Customs Service was transferred to the control of the Secretary acting through the Under Secretary. The Secretary is responsible for “[p]reventing the entry of terrorists and the instruments of terrorism into the United States,” “[s]ecuring the borders . . . [and] [e]stablishing and administering rules . . . ,” and for “ensuring the speedy, orderly, and efficient flow of lawful traffic and commerce.” As the Department of Homeland Security was taking office, the Administration used the authority provided to the Secretary to divide the Customs Service and the Bureau of Border Security. The two new bureaus within the Border and Transportation Security Directorate of the Department of Homeland Security are the Customs and Border Protection and the Immigration and Customs Enforcement (ICE). Both bureaus have broad authority to conduct searches of individuals crossing U.S. borders and share many of the same functions; Congress has even held hearings to discuss whether the two bureaus should be combined.

In 2007, the Department of Homeland Security stopped requiring any reasonable suspicion before border officials could conduct searches of travelers’ electronic devices. After a large public outcry demanding the DHS be more transparent in its border searches, on July 16, 2008, the CBP and the ICE made their respective policies regarding searches of electronic devices public. Both CBP Policy

39. See Bector, supra note 27, at 709.
44. Id.
45. See id. at 11.
47. Id.; see Bector, supra note 27, at 709.
and the ICE Directive gave officials unlimited discretion to search and retrieve files from any electronic device carried by passengers entering the U.S., exiting the U.S., or even passing through the U.S.\(^\text{48}\) In searching and reviewing detained or seized information, officials were subject to the limitation that the searches be completed in a "reasonable time."\(^\text{49}\) While the ICE Directive gave factors for ICE Special Agents to consider in determining a reasonable time,\(^\text{50}\) the CBP Policy did not define a reasonable period of time.\(^\text{51}\) Furthermore, if officials encountered probable cause of any unlawful activity, both policies allowed officials to seize and retain the originals or copies of the electronic media.\(^\text{52}\)

Both the CBP Policy and the ICE Directive provided for return of seized devices or destruction of copied information when no probable cause was found, but did not give a time when the return or destruction should occur.\(^\text{53}\) The CBP Directive provided some rules for assistance of other federal agencies in searches,\(^\text{54}\) and the ICE Directive provided similar rules for assistance from federal and non-federal agencies.\(^\text{55}\)

D. Congress Recognized the Conflict Between Travelers' Privacy Interests and the Government's Interest in Border Searches of Electronic Devices

The privacy interest at stake in the 2008 CBP Policy Regarding Border Search of Information and the 2008 ICE Directive for Border Searches of Documents and Electronic Media caught the attention of many, including Congress. Four bills were drafted in 2008 and early 2009 that proposed solutions by imposing regulations on searches of


\(^{50}\) 2008 ICE Directive, supra note 48, § 8.3.

\(^{51}\) Bector, supra note 27, at 709.

\(^{52}\) 2008 ICE Directive, supra note 48, § 8.5; 2008 CBP Policy, supra note 48, § D.

\(^{53}\) See 2008 ICE Directive, supra note 48, § 8.1; 2008 CBP Policy, supra note 48, § C.

\(^{54}\) 2008 CBP Policy, supra note 48, § C(2).

electronic devices and media at the borders.

1. Electronic Device Privacy Act of 2008

On July 23, 2008, Congresswoman Zoe Lofgren introduced the Electronic Device Privacy Act. The Act prohibited any person acting under the sovereign authority of the United States from searching a laptop computer or similar electronic device at borders. The problem with this act was its great breadth. The act was politically unfavorable because it did “not confer any authority to the United States border officials to investigate non-routine scenarios based on reasonable suspicion.”


On September 11, 2008, Congresswoman Loretta Sanchez introduced the Border Security Search Accountability Act of 2008. The Act required the Department of Homeland Security to issue rules regarding border searches of electronic media. The Act would require these rules to provide that commercial information be handled according to the laws, regulations, or rules governing such information, and that searches be performed in the presence of the official’s supervisor and the traveler. The Act would further require proper lengths of time for retention of information and individual notification if such information is put into a database. Individuals subject to search would also receive receipt if a device is seized, and an individual subject to border search would receive information regarding how to report abuses or concerns related to the search. Furthermore, information on traveler’s rights regarding border searches would be required to be posted at all ports of entry, and both a privacy impact assessment and a civil rights impact assessment of the rules would be required. While this bill did not pass the 110th

---

58. Bector, supra note 27, at 713.
61. H.R. 6869.
62. Id.
63. Id.
Congress, it has been reintroduced in the 111th Congress.64

3. Travelers’ Privacy Protection Act of 2008

In September 2008 Mr. Russ Feingold introduced the Travelers’ Privacy Protection Act of 2008.65 The Act incorporated many elements of the previous acts and added more detail, but only covered law abiding citizens and legal residents of the U.S.66 The Travelers’ Privacy Protection Act of 2008 required reasonable suspicion to search electronic devices, and either a warrant or an Order from the Foreign Intelligence Surveillance Court to seize an electronic device.67

The Act set specific procedures for the searches that included requiring the details be recorded, permitting the resident to remain present during the search, limiting the number of officials present to two, and requiring the search be tailored to the reasonable suspicion recorded prior to the search.68

The Act also set forth specific procedures for seizures of electronic devices after the initial search including when disclosure of the information to other agencies is appropriate, when the information should be destroyed, and when the resident should be provided with a receipt, statement of rights, and contact information for appropriate officials in the DHS.69

Additionally, the Act prohibited profiling in selecting residents for searches, provides compensation measures for damages due to search, and enables civil actions for violations of the bill.70


---

67. S. 3612; see Nojeim, supra note 36.
68. S. 3612; see Bector, supra note 27, at 715.
69. S. 3612.
70. Bector, supra note 27, at 715.
that to search the contents of an individual’s electronic device at the U.S. border, the search must be based on reasonable suspicion of the person. \(^72\) Also, the Act prohibits seizure of the device without constitutional authority beyond the power of the United States to search a person. \(^73\) Upon the traveler’s request, the search is to be made out of public view, and individuals may be required to turn on electronic devices to demonstrate operation. \(^74\)

Furthermore, the Act requires the Department of Homeland Security to promulgate regulations on searches of electronic devices including “policies for protecting the integrity of the data,” “policies for the length of time seized data will be stored and where and how it will be stored,” policies for sharing of downloaded information, information regarding return of device or media, and a requirement that a receipt be given to the traveler. \(^75\) The Act requires these policies be posted on the Department of Homeland Security’s website. \(^76\)

Additionally, the Act requires the United States Customs Service to conduct an annual study of searches and seizures of the previous year and report the findings to Congress annually. \(^77\) The study would include “the digital contents of digital electronic devices and digital storage media, and of seizures of such devices and media, that are based on the power of the United States to search or seize a person and that person’s possessions upon entry into the United States.” \(^78\) The study would also include the number of such searches and seizures; the types of searches conducted; the results of the searches; and the race, gender, and national origin of the travelers subject to those searches. \(^79\)

### III. DEPARTMENT OF HOMELAND SECURITY’S NEW DIRECTIVES ANNOUNCED AUGUST 2009

After being sued by the American Civil Liberties Union in early August 2009, \(^80\) seeing the public’s objections to the July 2008 CBP

\(^{72}\) Kim, *supra* note 6.


\(^{74}\) H.R. 239.

\(^{75}\) Id.

\(^{76}\) Bector, *supra* note 27, at 714.

\(^{77}\) H.R. 239.

\(^{78}\) H.R. 239.

\(^{79}\) Bector, *supra* note 27, at 714.

\(^{80}\) Chloe Albanesius, *ACLU Sues DHS over laptop searches*, PCMAG.COM, Aug. 26,
Policy and to the July 2008 ICE Directive,\textsuperscript{81} and seeing Congress’ proposed legislation to regulate border searches of electronic devices and electronic media, the DHS finally took action. On August 18, 2009, the DHS released new directives for the ICE,\textsuperscript{82} and on August 20, 2009, the DHS released new directives for the CBP.\textsuperscript{83} The new Directives dictate the rules for searches conducted by the officials under each department.\textsuperscript{84} They give more rules and standards to be implemented than the 2008 rules and incorporate many ideas from the proposed legislation.\textsuperscript{85} The new Directives, however, do not go far enough to reach an appropriate balance between travelers’ privacy interests and the Government’s interest in protecting our nation’s borders.

\textit{A. Analysis of the New Directives}

1. Technology Covered, Supervision of Search, Traveler’s Right to be Present

Both new Directives cover “any device that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices.”\textsuperscript{86} Neither Directive requires individualized suspicion to search electronic devices.\textsuperscript{87}

Similar to the recommendations in the proposed legislation,\textsuperscript{88} the 2009 CBP Directive states that searches of electronic devices should
be conducted in the presence of a supervisor.\textsuperscript{89} The ICE Directive does not have a similar requirement.\textsuperscript{90}

Unlike the 2008 CBP Policy and the 2008 ICE Directive, both 2009 Directives address what information the traveler should be given regarding the search and the presence of the traveler during the search.\textsuperscript{91} The CBP Directive states that the searches should be conducted in the “presence” of the traveler unless there is a “national security, law enforcement, or other operational consideration” that makes the traveler’s presence inappropriate.\textsuperscript{92} The CBP Directive then goes on to state that the traveler may be notified if a search is conducted, the purpose of the search, the authority for the search, and ways to find information on reporting concerns and redress if aggrieved by the search only if “the fact of conducting this search can be disclosed to the individual transporting the device without hampering national security or law enforcement or other operational considerations.”\textsuperscript{93} Similarly, the ICE Directive states, “[t]o the extent practicable, border searches should be conducted in the presence of, or with the knowledge of, the traveler.”\textsuperscript{94} “Not practicable” is described as times when there are law enforcement, national security, or other operational concerns.\textsuperscript{95}

Thus, the Directives provide that the traveler be notified of a search of his electronic device and possibly even be present for the search as long as a national security, law enforcement or operational concern is not identified.\textsuperscript{96} This is an expansive exception that can be fulfilled by many excuses; for example an “operational concern” exception can encompass a situation where officials do not have time to notify the traveler of the search because they were rushed to change


\textsuperscript{90} See 2009 ICE Directive, supra note 2.


\textsuperscript{93} 2009 CBP Directive, supra note 2, § 5.3.1.3.

\textsuperscript{94} 2009 ICE Directive, supra note 2, § 8.1(2).

\textsuperscript{95} Id.

\textsuperscript{96} See 2009 ICE Directive, supra note 2; 2009 CBP Directive, supra note 2.
shifts.\textsuperscript{97}

Even if the traveler is permitted to be present for the search of his device, both Directives state that permitting the traveler to be present for the search does not mean that the traveler may witness the search itself, if witnessing “could reveal law enforcement techniques, or potentially compromise other operational considerations.”\textsuperscript{98} Again, this exception is extremely broad. “Law enforcement techniques” and “other operational considerations” can encompass nearly any excuse given by a DHS official. A law enforcement technique can include which files on travelers’ devices officials examine first. Thus, a traveler permitted to be “present” for the search will likely not know exactly what information was searched because “witnessing” the search may “reveal law enforcement techniques or compromise other operational considerations.”

2. Detention of Electronic Device or Copies Thereof

Under both new Directives, officials may detain electronic devices or copies of electronic media for a “reasonable” time in order to complete a thorough search.\textsuperscript{99} Unlike the July 2008 CBP Policy and the 2008 ICE Directive, the new Directives provide a maximum amount of time that devices or copies of information can be detained before extensions are required.\textsuperscript{100} The CBP Directive states that such detention should not exceed five days.\textsuperscript{101} The ICE Directive states that such detention should not exceed thirty days.\textsuperscript{102} There is a significant difference in limits for “reasonable” lengths of searches under the two Directives, with no explanation as to why reasonable searches are limited to five days for the CBP and thirty days for the ICE. While the ICE has a longer time period allocated for searches before approval is required, the 2009 Directive, like the 2008 ICE Directive, lists factors to help determine a reasonable time for detention and completion of the search.\textsuperscript{103} The CBP Directive does

\textsuperscript{97} See id.
\textsuperscript{98} 2009 CBP Directive, supra note 2, § 5.1.4; 2009 ICE Directive, supra note 2, § 8.1(2); see Albanesi, supra note 87.
\textsuperscript{100} See 2009 ICE Directive, supra note 2; see 2009 CBP Directive, supra note 2.
\textsuperscript{101} 2009 CBP Directive, supra note 2, § 5.3.1.1; Timmer, supra note 92.
\textsuperscript{103} 2009 ICE Directive, supra note 2, § 8.3(3); 2008 ICE Directive, supra note 48, §
not include any factors to determine the length of a reasonable search.104

The 2009 Directives also set forth more specific requirements for approval of detention extensions. Extensions under both Directives can be obtained with approval.105 Under the ICE Directive, extensions can be granted in increments of fifteen days.106 The CBP Directive allows extensions beyond five days but requires further approval to extend the search past fifteen days.107

The limits on the duration of searches are additions from the 2008 CBP Policy and the 2008 ICE Directive.108 While the limits provide more concrete regulation of officials conducting searches and effectively limit the discretion of individual officials, the time periods of five days (in the case of CBP officials) and thirty days (in the case of ICE officials) with the ability to extend upon necessary approval still yield vast discretion to officials in border searches of electronic devices.109 The ICE Directive provides officials a much longer time for searches and allows for longer extensions than the CBP Directive.110 Both 2009 Directives state that “[w]hen CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation. . . , ICE policy will apply once it is received by ICE.”111 Therefore, the more liberal ICE policies apply to searches conducted by the CBP when the CBP turns the devices or copied information over to the ICE for analysis and investigation.112 The Directives state that the ICE and the CBP have “concurrently-held border search authority,”113 indicating that no individualized suspicion is required before the CBP can send the ICE detained, seized, or retained information.

Furthermore, travelers may not be aware that their electronic information was copied and the search continued if their device is

8.3(3).

105. See 2009 ICE Directive, supra note 2, ¶ 8.3(1); 2009 CBP Directive, supra note 2, ¶ 5.3.1.1.
106. 2009 ICE Directive, supra note 2, ¶ 8.3(1).
107. 2009 CBP Directive, supra note 2, ¶ 5.3.1.1; Timmer, supra note 92.
110. See id.
112. See id.
returned. The DHS Privacy Impact Assessment of the 2009 Directives explains, "[t]here is no specific receipt given to the traveler if the contents of the device are detained for further review, but the device is returned to the individual."\textsuperscript{114}

Depending on which bureau is conducting the search, supervisory approval may or may not be required before such a copy is made.\textsuperscript{115} The Privacy Impact Assessment explains times when copying information from a device without the knowledge of the traveler may be appropriate:

Copying may take place where CBP or ICE does not want to alert the traveler that he is under investigation; where facilities, lack of training, or other circumstances prevent CBP or ICE from performing the search at secondary inspection; or where the traveler is unwilling or is unable to assist, or it is not prudent to allow the traveler to assist in the search (such as providing a password to log on to a laptop).\textsuperscript{116}

Thus, copies of information on electronic devices can be made without the traveler’s knowledge and the search continued, as long as the original device itself is returned to the traveler.

3. Assistance from Other Agencies

Like the July 2008 CBP Policy, the CBP Directive allows other federal agencies to assist with technical difficulties presented in a search, foreign language difficulties, and encryption issues, including decrypting passwords or otherwise not readily reviewable material without any requirement of reasonable suspicion.\textsuperscript{117} Thus, the electronic device or copies of the information within can be sent to other federal agencies with or without reasonable suspicion.\textsuperscript{118} Before subject matter assistance may be requested from another federal agency, both the 2008 CBP Policy and the 2009 CBP Directive


\textsuperscript{115} 2009 CBP Directive, supra note 2, § 5.3.1.1; see 2009 ICE Directive, supra note 2 (While the 2009 CBP Directive provides that CBP officials must have supervisory approval to make copies, the ICE Directive does not have a similar requirement).


\textsuperscript{118} 2009 CBP Directive, supra note 2, § 5.3.2.2.
require that CBP Officers "have reasonable suspicion of activities in violation of the laws enforced by the CBP."\textsuperscript{119}

The 2009 ICE Directive, like the July 2008 ICE Directive, allows assistance from even non-federal agencies in translation, decryption, and other technical assistance with or without reasonable suspicion.\textsuperscript{120} Assistance from federal and non-federal agencies may also be requested for subject matter assistance if ICE Special Agents have reasonable suspicion of activities in violation of the laws enforced by the ICE.\textsuperscript{121} As discussed above, since the CBP can send information to the ICE and then ICE policy will apply to the search, the CBP can send detained traveler information to the ICE and then the ICE can send the information to non-federal agencies.\textsuperscript{122}

4. Destruction of Copied Information from Electronic Devices

Both the 2008 CBP Policy and the 2009 CBP Directive require destruction of copies if there was no probable cause to seize the electronic media and return of the device.\textsuperscript{123} The 2009 CBP Directive states that such information should be destroyed no later than seven days after the determination that there was no probable cause to seize, and unless circumstances require additional time not to exceed twenty-one days.\textsuperscript{124}

The ICE Directive gives seven business days for destruction of copied information from electronic devices after the determination that the information is "of no relevance to ICE."\textsuperscript{125} What is of no relevance to the ICE is not elaborated upon.

5. Retention and Seizure with Probable Cause

The July 2008 CBP Policy, the July 2008 ICE Directive, and the 2009 ICE Directive all allow seizure and retention of the electronic device or copy of information thereof if there is "probable cause of

\textsuperscript{119} See 2009 CBP Directive, supra note 2, § 5.3.2.3; 2008 CBP Policy, supra note 48, § C(2)(b); see Albanesius, supra note 80.

\textsuperscript{120} See 2009 ICE Directive, supra note 24, § 8.4(1); 2008 ICE Directive, supra note 48, § 8.4(1); see Timmer, supra note 92.

\textsuperscript{121} 2008 ICE Directive, supra note 48, § 8.4(2); see 2009 ICE Directive supra note 2, § 8.4(2).

\textsuperscript{122} 2009 CBP Directive, supra note 2, § 2.7; 2009 ICE Directive, supra note 2, § 6.2.

\textsuperscript{123} 2009 CBP Directive, supra note 2, §§ 5.3.1.2, 5.4.1.6; 2008 CBP Policy supra note 48, § C(1).

\textsuperscript{124} Albanesius, supra note 80.

\textsuperscript{125} 2009 ICE Directive, supra note 2, § 8.5(1)(e).
unlawful activity—based on a review of information in the electronic devices or on other facts and circumstances . . . .”126 In contrast, the 2009 CBP Directive allows retention of an electronic device or copies thereof only when there is probable cause to believe the device or copied information “contains evidence of or is the fruit of a crime that the CBP is authorized to enforce.”127 Thus, under the 2009 ICE Directive, if after searching a traveler’s electronic device the official has probable cause of any unlawful activity, the device may be seized and retained.128 As discussed above, even though the CBP may not have authority to seize a device, a CBP official can send the device or copy of electronic information to an ICE official who can then, under its policy, seize the device for probable cause of any unlawful activity.129

Once seized or retained, both the 2008 and 2009 Directives allow sharing of the information in accordance with applicable law and policy.130 Thus, under the 2009 ICE Directive, the ICE can seize or retain any device or copy of information with probable cause that the information contains or concerns any unlawful activity and then share that information with federal, state, and local law enforcement agencies in compliance with applicable laws.

6. Safeguarding Data During Storage and Transmission

Both new Directives, unlike the July 2008 CBP Policy, provide that the retained, copied, or seized information from electronic devices will be kept safe, and its locations documented.131 Both new Directives also require any suspected loss or compromise of information to be reported to a specified authority immediately.132

126. 2009 ICE Directive, supra note 2, § 8.5(1)(a); 2008 CBP Policy, supra note 2, § D(1)(a); 2008 ICE Directive, supra note 2, § 8.5(1)(a); see also John Timmer, supra note 92.
127. 2009 CBP Directive, supra note 2, § 5.4.1.1.
7. Privileged or Other Sensitive Materials

Both 2009 Directives as well as the 2008 CBP Policy and 2008 ICE Directive provide special provisions for sensitive information such as information that is attorney-client or attorney work-product privileged, medical records, information carried by journalists, business or commercial information, and other information protected by law.\textsuperscript{133}

These provisions likely do not adequately protect all privileged or other sensitive materials crossing the border. Both 2009 Directives add a provision that if officials suspect legal documents or those claimed to be attorney-client privileged “constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction” of the bureau searching (either the CBP or the ICE), then advice from the appropriate office must be sought.\textsuperscript{134} This provision likely does not guarantee protection of attorney-client privilege. Furthermore, U.S. domestic and international corporations and businesses send employees across its borders daily. The provisions in the 2009 Directives likely do not adequately protect the privileged information that is stored within the devices of those business travelers.

IV. PROPOSED SOLUTIONS TO THE IMBALANCE BETWEEN THE GOVERNMENT’S INTERESTS AND TRAVELERS’ PRIVACY INTERESTS AT THE BORDER

While the new Directives are an improvement over the past policies, they are largely the same as past policies\textsuperscript{135} and do not strike the DHS’s claimed “balance between respecting civil liberties and

\textsuperscript{133} See 2009 ICE Directive, supra note 2, § 8.6; 2009 CBP Directive, supra note 2, § 5.2; 2008 ICE Directive, supra note 48, § 8.7; 2008 CBP Policy, supra note 48, § E; see also Albanesius, supra note 80.

\textsuperscript{134} 2009 ICE Directive, supra note 2, § 8.6(2)(b) (stating “[i]f Special Agents suspect that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of ICE, the ICE Office of the Chief Counsel or the appropriate U.S. Attorney’s Office must be contacted before beginning or continuing a search of the document and this consultation shall be noted in appropriate ICE systems.”); 2009 CBP Directive, supra note 2, § 5.2.1 (stating “[i]f an Officer suspects that the content of such a material may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP, the Officer must seek advice from the CBP Associate/Assistant Chief Counsel before conducting a search of the material, and this consultation shall be noted in appropriate CBP systems of records. CBP counsel will coordinate with the U.S. Attorney’s Office as appropriate.”).

One of the biggest problems with both the 2008 and 2009 versions of the DHS Directives is that they are written with ambiguous terms leaving travelers confused about what to expect when crossing the U.S. border with electronic devices or electronic media. For example, travelers may or may not have their electronic devices searched depending on the whim of an ICE or CBP official. Travelers subjected to a search of their electronic device may or may not be able to watch or even be present for the search, their information may or may not be copied and retained and even sent to other federal or non-federal agencies, and their electronic device or media may be seized upon probable cause of unlawful activity depending on which bureau conducted the search. While these ambiguities leave travelers feeling somewhat helpless, they also work to protect U.S. borders from terrorists and contraband. Rules regulating border searches need to reach a better balance between the government’s interest in protecting the borders and traveler’s privacy interests.

A. Reasonable Suspicion Should be Required

There is a valid argument that because electronic data does not need to cross the border through a physical device to be transmitted inside, outside, or to pass through the country, there is no special need for the government to search such information at the border. This argument reasons that data can be electronically transmitted and received between the United States and other countries through e-mail, internet-postings, etc.; thus, any right that the government has to search your laptop for such information at the U.S. border is the same right that it has to search your laptop while located anywhere inside the country. Because suspicion is required for searches of

137. Erwin Chemerinsky, Laptop Search at Border Was Illegal, Los Angeles Daily Journal, Nov. 29, 2006, at 6 (reasoning that:
The government has no special interest at the border in searching a person’s computer different from computers that are already in the country. The government is allowed to engage in suspicionless border searches where there is an interest unique to the border, such as preventing people from entering illegally or in intercepting drugs or weapons being brought into the country. But these interests do not exist with regard to the memory of computers.).
electronic devices when the person is inside the country, and a person’s privacy interest is the same while inside the country as at the border, it is logical that reasonable suspicion be required for searches of electronic devices at the border.  

Furthermore, searches of electronic devices at the border monopolize valuable time of ICE Special Agents and CBP Officials. Searches of electronic devices are lengthy because the official must first initiate the search, and if the official is a CBP agent, then this official must obtain supervisor approval. The official must then turn on the device and complete a thorough search while following the required recording, searching, and documenting protocols. This procedure is an especially inefficient allocation of resources when the search is without any reasonable suspicion, and other travelers are passing through border checkpoints with less scrutiny.

Additionally, great discretion in the hands of border officials leads to profiling. If reasonable suspicion is not required to conduct border searches of electronic media, the decision regarding whose devices to search is left to the whims of individual officials, and searches may fall on people they decide look untrustworthy. Such whims can include various profiling reasons, the official’s personal interest, or even to harass a difficult traveler. Reasonable suspicion, or “one good reason” as proposed by one scholar, should be required to at least limit searches from being conducted for illegitimate and profiling reasons.

B. Congress Should Require the DHS to Conduct an Annual Study of the Searches, Report the Results to Congress, and Promulgate New, More Definite, Directives Based on the Findings

I propose that Congress require the DHS to conduct an annual study and report the findings to Congress, similar to the study requirement proposed in the Securing Our Borders and Our Data Act

139. Id. at 255.
140. See Fontecchio, supra note 4, at 248.
141. 2009 CBP Directive, supra note 2, §5.1.3.
143. Fontecchio, supra note 4, at 251-52.
144. Id. at 254.
145. Id. at 264-265.
of 2009.146 The study should include the number of searches conducted, what devices and electronic media were searched, how long the searches took, how often the official’s supervisor was in the room, how often travelers were permitted to be present during the search, how often travelers were permitted to witness the search, which officials were present for the search, how many devices and copies of electronic media were detained, when passwords were decrypted, techniques used to search, if a federal or non-federal agency assisted in the search, how many devices or copies of electronic information were seized, as well as the race, gender, and national origin of the travelers subject to those searches. The study should also include the overall result of the search, mainly whether unlawful activity was prevented and the type of unlawful activity prevented.

The DHS should then be required to annually update and reissue the Directives based on the results of the study. Through annual analysis of the searches of electronic devices and electronic media, the DHS will remain acutely aware of the realities of the searches and the privacy interests at stake. Congress and the DHS should be able to tailor the amount of discretion in the hands of border officials to sufficiently meet the government’s interest while also accommodating travelers’ privacy interests. Furthermore, the yearly report to Congress will hold the DHS responsible for any abuses in conducting border searches of electronic media and will allow Congress to take action if it believes the DHS Directives are insufficient or inappropriate.

Analysis of the annual studies should reveal whether it is ever appropriate for travelers to witness the searches; or in the case that they do witness the searches, which “law enforcement techniques” or “other operational considerations” should be sufficient to prevent them from witnessing the search. The annual studies may also reveal what electronic devices are most commonly used for transporting illegal information, and should therefore be searched most often. Comparison of the ICE and CBP study results may reveal whether the presence of the official’s supervisor during the search is preferable, whether the ICE reasonableness factors should be incorporated into the CBP’s policies, and whether allowing electronic information to be sent to non-federal agencies for either technical or subject matter

---

assistance is desirable.

The CBP and ICE policies should evolve to be more similar because the two bureaus have "concurrently-held border search authority," conduct similar searches, and the CBP can send any detained device or copy of information to the ICE and the ICE policies will then apply. Annual updating and refining of the directives should facilitate the evolution of directives with less discrepancy between the appropriate time for searches of electronic information and approval requirements for extensions between the two bureaus. The time regulations should be tailored to accurately reflect the actual reasonable time required by the ICE and CBP to conduct thorough searches. Continuous refining will allow the directives to reach an appropriate balance between the government’s interest in conducting border searches of electronic devices and travelers’ privacy interests.

C. Travelers Should Be Better Warned of the Great Discretion Afforded Border Search Officials Before They Get to the Airport

Most travelers are unaware when they travel internationally through U.S. borders that their electronic devices may be searched, detained for numerous days, and even sent to other federal agencies without any individualized suspicion of unlawful activity. Most travelers are also unaware that if an ICE official has probable cause of any unlawful activity on an electronic device, the device may be seized. If border officials are to have such great discretion in searching electronic media at the borders, then the government should make travelers better aware of the policies regarding border searches of electronic devices.

Provisions to put the public on notice of the Department of Homeland Security's broad authority to search electronic devices at the borders are limited to: the Directives posted on the DHS website, signs posted at the entrance of port areas, various Systems of Record Notice (SORNs) published in the Federal Register regarding retention information from travelers' electronic devices at the border, and "tear sheets" provided when devices are detained or seized. While the

150. See Hoffman, supra note 16, at 182.
151. Dep’t of Homeland Sec., Privacy Impact Assessment CBP and ICE Border Searches
Directives themselves are posted on the DHS website to notify travelers of the DHS's broad authority to search electronic devices, most travelers do not know to look at the website because they have no idea that such searches are possible.

The DHS's Privacy Impact Assessment explains that the CBP is working to amend signs at the entrance of port areas "to state explicitly that electronic devices are subject to detention and search, and to include a Privacy Act Statement providing notice of DHS’s authority to collect information from electronic devices." The SORNs published in the Federal Register provide information about the types of records maintained, information about seizures, fines, penalties, etc., and information about seized or detained information.

The Privacy Impact Assessment also explains that a "tear sheet" will be given to travelers whose devices are detained or seized, the sheet "containing information concerning the CBP/DHS’s authority to perform its search, detention, and possible seizure." While the signs, Directives posted on the D.H.S website, SORNs published in the Federal Register, and the tear sheets aid in informing travelers of the DHS's broad authority, they do not adequately warn travelers before travelers depart for the airport to travel internationally.

To give travelers better notice, Congress should require airlines to post notices describing the DHS's authority to search electronic devices at the border within the airline ticket purchasing process before a ticket is purchased, on the airline ticket itself, and on the airline's website. Many travelers glance through the notices presented when purchasing airline tickets, visit the airline website while packing for their trip (to check what may or may not be brought in carry-on luggage, etc.), and look over their airline tickets. These notices should inform travelers of the possibility that their electronic devices may be searched without individualized suspicion, detained for numerous days, sent to other federal agencies and possibly non-federal agencies, and even seized if an official has probable cause of any illegal activity, including trademark and copyright violations. The notices

---

152. Id.
should also explain that the DHS can recover deleted files and unencrypt encrypted files. If travelers are aware of the DHS’s power to search their electronic devices and electronic media, they can take steps to safeguard their own privacy interests before leaving for the airport to travel internationally.

V. Conclusion

The “border search” exception to the Fourth Amendment holds “routine searches” as reasonable and thus requires no individualized suspicion. As courts currently deem searches of electronic devices to be “routine,” such searches do not require individualized suspicion. These searches implicate travelers’ privacy interests because electronic devices contain immense amounts of highly personal and private information. The Department of Homeland Security’s August 2009 Directives on border searches of electronic devices and electronic media impose more regulations on these searches than past policies, but are still vague and contain wide exceptions. Analysis of these Directives indicates that the DHS has yet to reach an adequate balance between the government’s interest in conducting border searches of electronic devices and traveler’s privacy interests.

To reach an adequate balance, at least some reasonable suspicion should be required before an electronic device is searched at the border. Since electronic information can be sent into and out of the country without being physically carried across the border in a device, there is no special need for the government to search such information at the border. Furthermore, requiring at least some suspicion will allow border officials to more efficiently allocate their time, and will prevent searches from being conducted for improper reasons.

To balance national security interests with the privacy interests of travelers, Congress should require the DHS to conduct an annual study of its searches, report the results to Congress, and issue refined directives based on the results of the study. The continual refining of the directives will allow the rules regarding searches of electronic media to change with the changing technology and to be tailored to protect privacy interests while leaving the officials discretion to protect homeland security.

Finally, Congress should require airlines to put notice of the DHS’s broad authority to conduct searches of electronic devices

157. United States v. Romm, 455 F.3d at 1006.
158. 2009 ICE Directive, supra note 2, § 8.4; 2009 CBP Directive, supra note 2, § 5.3.2.2.
within their ticket-purchasing process, on their websites, and on the airline tickets themselves. This measure will better ensure that travelers are aware of the DHS’s authority to search their electronic devices at the border and allow travelers to take adequate steps to protect their privacy interests.