Civil Rights/Civil Liberties Impact Assessment

Border Searches of Electronic Devices

December 29, 2011

Reviewing Official:
Margo Schlanger
Officer for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
(202) 357-7765

Table of Contents

I. Introduction **1**
II. Facts **4**
A. Primary Inspection and Referral 4
B. Secondary Inspection and Electronic Device Searches 6
III. Legal and Policy Analysis **9**
A. Authority to Search Electronic Devices at the Border 10
B. First Amendment 17
C. Equal Protection and Religious/Ethnicity Discrimination 18
D. Time Limits 20
E. Privileged Materials 21
F. Improved Notice about Redress 22
IV. Conclusion **22**

I. Introduction

This Civil Rights/Civil Liberties Impact Assessment, conducted by the Office for Civil Rights and Civil Liberties (CRCL) of the Department of Homeland Security (DHS), focuses on the Department's policies guiding the border search of electronic devices, how those searches occur, and related civil rights and civil liberties issues. Without finding any existing constitutional violation in policy or practice, we make several recommendations to further safeguard travelers' civil rights and civil liberties with respect to electronic device searches by improving accountability and oversight structures, and providing better notice to travelers about the availability of redress if they have complaints related to such searches.

The issue is an important one, even though it affects only a very small proportion of the many millions of travelers who enter the United States each month. The table below summarizes the relevant statistics; as it shows, only a few hundred people each month are subjected to any kind of electronic device search (which vary in their comprehensiveness), and of that number, only a small minority have their electronic devices detained for any length of time.

Table: CBP Electronic Device Searches—Number Impacted

	Monthly Averages	
	FY 2009	FY 2010
Travelers through all Ports of Entry	21,641,667	29,357,163
Travelers in Secondary Screening	466,667	518,059
Travelers Subjected to Electronic Device Searches	302	383
Detentions or Seizures of Electronic Devices	25	16

Notwithstanding the low rate of searching, we recognize that for the several thousand people affected each year, electronic devices searches may pose a significant concern. In August 2009, Secretary Napolitano announced revised U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP) policies with respect to searches of electronic devices in response to public and congressional concern, and as part of the continuing evolution of border security policy. At the same time, the Secretary directed that CRCL assess the impact of these policies, to ensure that civil rights and civil liberties concerns are appropriately addressed and to look for ways in which the new policies might be improved. For this resulting Civil Rights/Civil Liberties Impact Assessment, we have reviewed the CBP and ICE policies guiding the border search of electronic devices; consulted with CBP and ICE personnel to understand implementation of the policies and ascertain how searches occur; and considered legal, policy, and practical concerns raised by advocacy groups and the public. Because border searches of electronic devices ordinarily occur only in conjunction with a secondary inspection, this Impact Assessment first briefly discusses the process by which CBP refers travelers to secondary inspection. It then focuses on the electronic device search policies and their implementation, describing the relevant legal authority and assessing the impact on individual rights. Finally, the Impact Assessment offers policy advice to Department and Component leadership about how to improve accountability, oversight, and notice about redress. This assessment does not address training. CBP's relevant training content and processes were the

subject of a separate review jointly conducted by the DHS Privacy Office, CRCL, and CBP, issued August 20, 2010, and available at http://www.dhs.gov/xlibrary/assets/privacy/privacy-report-cbp-training-border-searches-electronic-devices.pdf.

In addition, CBP's Office of Internal Affairs, Management Inspection Division (MID), conducted its own review of CBP's electronic device search policies. That review, completed in November 2010, found that while CBP officers were executing searches of electronic devices and documents with appropriate care and infrequency, there were some conditions warranting additional attention. Specifically, and relevant to the current analysis, MID found that:

1) CBP's system for entering the results of electronic device searches did not allow analysts to accurately identify incidents and seizures related to electronic device search activity, thus hindering CBP's ability to monitor and evaluate performance and making it difficult to provide accurate operational data concerning searches of electronic devices;
2) some CBP supervisors and officers were confused about their obligation to track information related to searches of electronic devices that had been transferred to ICE for forensic analysis versus those that had been transferred to ICE for translation or encryption services;
3) many supervisors and officers incorrectly believed that supervisory approval was required for device searches, and this belief hindered CBP's enforcement mission by discouraging officers from searching electronic devices; and
4) many supervisors interpreted CBP's supervisory presence requirement to require only that a supervisor be somewhere in the general area, not that a supervisor be physically present for the search.[1]

CBP addressed concerns (2)-(4) to MID's satisfaction in a Muster issued in October 2010[2] and is in the process of amending data systems to address the first concern. We discuss the relevant provisions of these CBP policies in detail and provide additional information regarding MID's findings and recommendations later in this report (*see infra* Part II.B.).

We note at the outset of this Assessment that two lawsuits currently pending before federal district courts concern some of the same issues considered in this Assessment. In *Abidor v. Napolitano*, No. 1:20-cv-04059 (E.D.N.Y. filed Sept. 7, 2010), the individual plaintiff alleges that he was searched on board an Amtrak train at the port of entry between Quebec and New York and that his laptop and external hard drive were detained for further inspection. The National Association of Criminal Defense Lawyers and National Press Photographers Association are also plaintiffs in the *Abidor* case. The plaintiffs allege that the individual search, and 2009 CBP and ICE policies, violate the Fourth Amendment by permitting the suspicionless search, copying, and detention of electronic devices and the First Amendment by permitting the suspicionless search, copying, and detention of electronic devices containing expressive materials. Complaint at 33, *Abidor v. Napolitano*. In *House v. Napolitano*, No. 1:2011cv10852 (D. Mass. filed May 13, 2011), the plaintiff states that he

[1] *See* Management Inspections Division, Office of Internal Affairs, U.S. Customs and Border Protection, Border Search of Electronic Devices and Documents, Report Number MID-10-003 (November 19, 2010) [hereinafter MID Report].

[2] U.S. Customs and Border Protection, Dep't of Homeland Sec., Muster, Border Search of Electronic Devices Directive 3340-049 (October 25, 2010) [hereinafter October 2010 Muster].

has been targeted for surveillance and investigation by various agencies of the U.S. government and alleges that a 2010 search and detention of his laptop, USB device, and video camera violated the First and Fourth Amendments. *See* Complaint at 9, *House v. Napolitano*. As explained below, we do not believe that the 2009 policies violate either the First or Fourth Amendment. *See* discussion *infra* Parts III.A.1-B.

ICE and CBP exercise longstanding constitutional and statutory authority permitting suspicionless and warrantless searches of merchandise at the border and its functional equivalent. But we conclude that the 2009 Directives impose useful requirements governing use of this authority in searching, reviewing, retaining, and sharing information contained in electronic devices. The management controls imposed on these activities include limitations on how long devices should generally be retained for completion of a border search, requirements that notice be provided the device owners regarding the process, and supervisory oversight to help prevent abuse of discretion by individual officers. To further protect the individual liberty of travelers, however, we make five recommendations, each related to the decision to conduct an electronic device search. All but one are directed only to CBP, because nearly all such decisions are made by CBP:

1. ***Rationale:* CBP officers who decide to conduct a device search generally should record the reason for the search in a TECS field. The reason should specifically relate to the decision to inspect an electronic device, not merely the selection for secondary screening (although the reason for both may be the same). To be clear, we are not recommending that officers demonstrate reasonable suspicion for the device search; rather we recommend that officers simply record the actual reason they are conducting the search, whatever that reason is. This recommendation exceeds constitutional requirements, but should facilitate CBP's operational supervision and oversight.**

2. ***Antidiscrimination Policy:* CBP and ICE should state explicitly in policy that it is generally impermissible for officers to discriminate against travelers—including by singling them out for specially rigorous searching—because of their actual or perceived religion, and that officers may use race, religion, or ethnicity as a factor in conducting discretionary device searches only when (a) based on information (such as a suspect description) specific to an incident, suspect, or ongoing criminal activity, or (b) limited to situations in which Component leadership has found such consideration temporarily necessary based on their assessment of intelligence and risk, because alternatives do not meet border security needs.**

3. ***Regular Monitoring:* CBP should improve monitoring of the distribution of electronic device searching by race and ethnicity, by conducting routine analysis, including annual examination of electronic device searches by port of entry. After controlling for known relevant and permissible factors, such as port traveler demographics, and (b) (7)(E) [redacted] (b) (7)(E) [redacted] the analysis should assess whether travelers of any particular ethnicity—estimated using nationality/country of birth and name analysis—at any port of entry are being chosen for electronic device searches in substantial disproportion to that ethnicity's portion of all travelers through the port. The analysis should also consider U.S. citizens separately from others. Data and results should be shared with CRCL.**

4. ***Subsequent Supervision:*** **If it appears that electronic device searching in any port has a substantial unexplained skew towards travelers of one or more ethnicity, CBP should work with CRCL on developing appropriate oversight mechanisms. Subsequent steps generally should include a requirement of supervisory approval for searches (absent exigent circumstances) or enhanced training, and may include other responses.**

5. ***Improved Notice:*** **CBP should improve the notice given to travelers subjected to electronic device searches by updating tear sheets to refer travelers to DHS TRIP if they seek redress.**

DHS is required by law to execute its border security mission in a manner that protects civil rights and civil liberties. The Department's authorizing statute explains that among the "primary mission[s] of the Department is to … ensure that the civil rights and civil liberties of persons are not diminished by efforts, activities, and programs aimed at securing the homeland." 6 U.S.C. § 111(b)(1) (2006). This requirement goes beyond simply ensuring minimal civil rights and civil liberties compliance. This Office and the Department as a whole are committed to building systems that protect civil rights and civil liberties in both policy design and practice, and to enhancing protections when there is no countervailing harm to the Department's law enforcement efforts. Our recommendations are in this spirit. They are intended as the Office for Civil Rights and Civil Liberties' advice to the Secretary, who requested this Impact Assessment, and do not purport to state the current position of the Department. Nor are the policy recommendations, in particular, intended to create any judicially enforceable rights or remedies.

II. Facts

A. Primary Inspection and Referral

Both ICE and CBP are charged with deterring, detecting, and apprehending the importation of contraband, enforcing laws controlling the flow of persons and goods across the borders, and assisting myriad other federal enforcement agencies when those agencies' enforcement activities have a border nexus. CBP is responsible for securing United States borders and determining the admissibility of all persons or goods seeking to travel across the border at 327 ports of entry; ICE, among its other responsibilities, is the agency that investigates criminal activity relating to border crimes. Together they confront illegal activity at the border to detect evidence relating to terrorism and other national security matters, as well as, for example, narcotics, human and bulk cash smuggling, contraband, and child pornography.[3] Congress has long recognized, and the Supreme Court has repeatedly affirmed, the importance of these missions and the broad authority ICE and CBP customs officers[4] have to protect our borders.[5] (Rather than distinguishing between CBP

[3] U.S. Customs and Border Protection, Dep't of Homeland Sec., Directive No. 3340-049, Border Search of Electronic Devices Containing Information (Aug. 20, 2009), *available at* http://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf [hereinafter CBP Directive]; U.S. Immigration and Customs Enforcement, Dep't of Homeland Sec., Directive No. 7-6.1, Border Searches of Electronic Devices § 4 (Aug. 18, 2009), *available at* http://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf [hereinafter ICE Directive].

[4] 19 U.S.C. § 1401(i) (defining "customs officer").

Officers and ICE Agents, this Impact Assessment uses "officer" as a generic description for the relevant CBP and ICE personnel.) As already summarized, the volume of the resulting ICE and CBP activities is vast: CBP encounters more than 22 million travelers each month at its 327 ports of entry. The range of contraband seized from these travelers runs a broad gamut. Officers search persons, goods, and commercial and personal containers for contraband, daily detaining on average 1903 individuals for illegal entry, making on average 75 criminal arrests, and seizing 11,435 pounds of illegal narcotics.[6] Although narcotics and weapons seizures are the interdictions that most frequently make headlines, and forbidden agricultural products are the most frequently seized items, contraband also include documents such as child pornography or fraudulent passports. Still other seized documents may not be contraband per se, but constitute evidence of crimes relating to terrorism, immigrant smuggling, immigration fraud, narcotics, trafficking, illegal technology transfer, financial crimes, and other crimes falling under DHS jurisdiction.[7]

The decision to search a traveler is based on the totality of information available to an officer; the immensity of the flow of travelers and goods into and out of the United States shapes CBP and ICE search policies and practices. Resources for performing detailed and time-consuming border searches, including laptop searches, are limited, making the efficient allocation of resources critical for officers and supervisors. For each traveler arriving at any port of entry—land, air, or sea—the first step is to undergo primary immigration examination and customs inspection. During the primary examination, a CBP officer asks questions to establish whether the traveler is admissible into the United States; if that determination cannot be made quickly, the passenger will be referred to secondary inspection. (For air and sea passengers, the process actually starts with prescreening—an (b) (7)(E) [redacted] f a traveler upon arrival, or to further evaluate admissibility of an alien.)

Officers performing primary inspection do not follow a set script, instead asking questions (b) (7)(E) [redacted] to support the discretionary decision to clear travelers directly from primary inspection or instead refer them to secondary inspection.

Referrals to secondary inspection may be made for any reason. Yet the techniques officers apply to make referral decisions channel their broad discretion (b) (7)(E) [redacted]

---

[5] *See United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) ("Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country.").

[6] U.S. Customs and Border Protection, Dep't of Homeland Sec., On a Typical Day in Fiscal year 2010, CBP … (Feb. 25, 2011) http://www.cbp.gov/xp/cgov/about/accomplish/typical_day_fy2010.xml.

[7] CBP Directive, *supra* note 3; ICE Directive, *supra* note 3.

(b) (7)(E) [redacted] These are described in the 2004 CBP *Personal Search Handbook*[8] and in CBP officer Primary Training, as well as in other procedural guidance and training documents. In addition to (b) (7)(E) [redacted] mentioned above, some referrals to secondary inspection may result from (b) (7)(E) [redacted] CBP also conducts a limited number of random compliance examinations, denominated "COMPEX" searches.[9] Nearly 98% of travelers are admitted/cleared into the United States directly from primary inspection. The small group for which this is not true are referred to secondary inspection, and may be subject to further interview, personal search, agricultural inspection or duties assessment, or more detailed baggage inspection—which can include search of electronic devices.

B. Secondary Inspection and Electronic Device Searches

CBP and ICE do not target electronic devices alone; such devices are one of many types of items or containers that may be searched, usually during secondary inspection. And an electronic device may be subjected to one or more types of scrutiny. These include:

- A brief physical inspection by an officer, including the traveler opening a case, or perhaps turning a device on, in order to demonstrate that the device is what it purports to be and not a container for tangible contraband (e.g., illegal drugs). This type of inspection is not considered to be an electronic device search for the purposes of the border search policy.[10]
- Search of the device's contents.
- Detention of a device, or of a copy of information contained on the device, for the completion of forensic examination. ICE and CBP policies provide guidance on the length of time electronic devices may generally be detained. The guidance is flexible in light of operational requirements, and differs between the two Components based upon their differing missions. Minimizing the length of time a device is detained is a goal of both policies, but encryption, large volumes of documents, password protections, and the need for computer forensic assistance may cause detention to last up to several months, and the policies deal with this delay in different ways, discussed immediately below.
- Seizure of a device as evidence of a crime, or for civil forfeiture under applicable law. A seized device is ordinarily retained through trial as evidence, subject to normal evidentiary handling rules. (If a device is subject to forfeiture, appropriate forfeiture proceedings are initiated as provided by law. *See* 19 U.S.C. §§ 1600-1617 (2006).)
- Retention of a device, or of a copy of information contained on the device, for evidence of continued or future admissibility.

[8] Office of field Operations, U.S. Customs and Border Protection, Personal Search Handbook (2004) [hereinafter Personal Search Handbook].

[9] *See* U.S. Customs and Border Protection, Dep't of Homeland Sec., Random Exams, http://www.cbp.gov/xp/cgov/travel/admissibility/random_exams.xml.

[10] CBP Directive, *supra* note 3, at § 3.4.

As the front-line law enforcement agency, CBP restricts more tightly than ICE does the length of time a device can be detained. If CBP detains a device for more than five days, a port director or equivalent manager must approve the detention extension, and any detention past 15 days requires approval from senior CBP management, such as the Director of the Office of Field Operations.[11]

ICE's role is to run longer-term investigations. If a device is turned over to ICE for such an investigation, ICE policy gives officers up to 30 calendar days to complete border searches without seeking supervisory approval. Searches exceeding 30 days are to be documented in ICE information systems, and must be approved by the relevant Group Supervisor, with continuing approval required every 15 days thereafter. To limit the length of time a device may be detained, ICE has identified specific factors to be considered by the investigating officer to ensure that the time taken to conduct the search is "reasonable" given the facts and circumstances of the particular search: (1) the amount of information needing review; (2) whether the traveler was deprived of his property and, if so, whether the traveler was given the option of continuing his journey with the understanding that his property would be returned once the border search was complete or a copy could be made; (3) the elapsed time between the detention, the initial border search, and the continued border search, including any demand for assistance; (4) whether the traveler has taken affirmative steps to prevent speedy search; (5) whether and when ICE or CBP followed up with the agency or entity providing assistance to ensure timely review; and (6) any unanticipated exigency that may arise.[12]

CBP and ICE policies both direct officers to conduct electronic device searches in the presence of the traveler unless there are special national security or operational considerations (such as preserving the integrity of an investigation) that would make it inappropriate for the traveler to observe the search.[13] Furthermore, for CBP, although express supervisory approval is not required, electronic device searches are to occur in the presence of a supervisor unless contacting a supervisor is not practicable, and in such instances the officer is required to notify a supervisor about the search and any results as soon as possible.[14] Several officers, both in the field and at Headquarters, have told CRCL that the supervisory presence requirement means, in practice (though not as a matter of national policy), that supervisors are asked to permit a search of an electronic device, and that supervisors may require an articulated reason for that search. As noted above, MID found a significant degree of confusion regarding the issues of supervisory presence and approval in the field. CBP has now clarified that supervisory approval is required only for detaining devices or copies of information contained therein, and that when performing a manual border search of an electronic device a supervisor need not be present or approve the search, although officers are advised that the better practice is to have a supervisor present during such searches.[15] ICE Special Agents are authorized to make investigative decisions based on the particular facts and circumstances of each case and do not require supervisory approval.[16]

---

[11] CBP Directive, *supra* note 3, at § 5.3.1.1.

[12] ICE Directive, *supra* note 3, at § 8.3.

[13] CBP Directive, *supra* note 3, at § 5.1.4; ICE Directive, *supra* note 3, at § 8.1.2.

[14] CBP Directive, *supra* note 3, at § 5.1.3.

[15] October 2010 Muster, *supra* note 2.

[16] ICE Directive, *supra* note 3, at § 6.1; ICE Special Agents are required to obtain supervisory approval for detentions that exceed 30 days (any detention exceeding 30 calendar days must be approved by a supervisor, and approved again every 15 calendar days thereafter).

For CBP searches, the fact of the search and information about it is recorded in the TECS system[17]; currently, information collected includes the general reason for the referral to secondary inspection and, in a "remarks" section, what was searched, and what, if anything, resulted from that search. Officers in both agencies are required to record any secondary examination of an electronic device[18] by completing an after-action report—including in TECS all information related to the search through the final disposition including supervisory approvals and extensions when appropriate—entered into TECS.[19] MID found, however, that these systems were inadequate. It recommended that CBP identify and implement actions required to ensure data extraction methods provide precise statistics on the number of searches, detentions, and seizures of documents and electronic devices recorded in TECS; and that CBP develop and implement a new TECS module, or enhance existing modules, to facilitate the accurate recording of electronic device search enforcement actions, allow for automatic notification of required supervisory approvals; and enable the tracking of detained documents and electronic devices.[20] CBP concurred with both of these recommendations and is in the process of implementing them.

When examining an electronic device, if an officer determines that probable cause exists to believe that the device contains evidence of violation of a law that CBP or ICE is authorized to enforce, officers may seize and retain the device, or may create and retain a copy of relevant information.[21] If the officer determines that there is no probable cause to seize the device or retain a copy, the device is returned to the traveler within seven business days of that determination, unless a supervisor authorizes an extension of up to 14 additional days.[22] If any information was copied, it is destroyed on the same schedule—except that even in the absence of probable cause, ICE or CBP may retain copied information that relates to immigration, customs, and other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained.[23]

During the course of a border search, ICE or CBP officers may discover that they need subject matter assistance to understand the significance of the information discovered, or technical assistance to translate or decrypt information on the device. While not required by law, both ICE and CBP policies require that requests for subject matter assistance from outside agencies be premised upon reasonable suspicion of activities in violation of the laws enforced by CBP and ICE. Requests for technical assistance, such as translation or decryption, are permitted without such a threshold showing.[24] CBP's policies state that a traveler's presence on the government-operated and

---

[17] TECS is a user interface that permits users to check and add to law enforcement-related database records about travelers. *See* 73 Fed. Reg. 77778 (Dec. 19, 2008).

[18] CBP Directive, *supra* note 3, at §5.5; ICE Directive, *supra* note 3, at § 8.2(2)-(3).

[19] CBP Directive, *supra* note 3, at § 5.5.1; U.S. Immigration and Customs Enforcement, Dep't of Homeland Sec., Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices (Dec. 12, 2008).

[20] MID Report, *supra* note 1, at 12-13.

[21] CBP Directive, *supra* note 3, at § 5.4.1.1; ICE Directive, *supra* note 3, at § 8.5(1)(a).

[22] CBP Directive, *supra* note 3, at § 5.3.1.2; ICE Directive, *supra* note 3, at § 8.5(1)(e).

[23] CBP Directive, *supra* note 3, at § 5.4.1.2; ICE Directive, *supra* note 3, at § 8.5(1)(b).

[24] CBP Directive, *supra* note 3, at § 5.3.2; ICE Directive, *supra* note 3, at § 8.4.

government-vetted watchlist is sufficient to support a determination of reasonable suspicion.[25] The October 2010 Muster notes the importance of documenting electronic device searches and clarifies the contrasting documentation requirements that apply when CBP transfers a device to ICE for subject matter assistance versus those that apply when ICE detains a device on its own authority.[26]

Once the requested assistance is provided to CBP or ICE, both require that all information shared with an outside agency be returned and copies be destroyed as expeditiously as possible, unless the assisting agency has independent legal authority to retain a copy of information, in which case both ICE and CBP request that the retaining agency notify ICE or CBP that it is retaining information.[27] CBP (but not ICE) policy requires that travelers be notified of any information sharing unless notice would be contrary to national security, law enforcement, or other operational interests.[28]

(b)(7)(E) [redacted] when CBP detains an electronic device, CBP provides each traveler whose electronic device is searched with a "tear sheet" listing the legal authority for the search of his electronic device and explaining some possible reasons why travelers may be selected for such a search, what the traveler should expect, and information regarding how to seek redress.[29] This form also provides information concerning DHS and CBP privacy policy, a web address for the DHS Office for Civil Rights and Civil Liberties, and contact information for the CBP Info Center. Additionally, whenever they detain or seize an electronic device, CBP and ICE provide the traveler with a chain of custody form.[30] If a device is detained, the traveler receives Form 6051D; if the device is seized, the traveler receives Form 6051S. These forms serve as notice and a receipt for seized/detained property.

III. Legal and Policy Analysis

This section examines the lawfulness of the CBP and ICE policies governing searches of electronic devices at the border, concluding that they do not violate the Fourth or First Amendments or the Equal Protection Clause. Nonetheless, although we conclude that these policies are lawful and represent marked improvement over past policies, the protection of civil rights and civil liberties is more than upholding a constitutional floor for government behavior. The Department's activities to enforce the laws and provide security necessarily involve detection and deterrence of crimes facilitated by electronic devices, and therefore require intrusion into aspects of people's lives that would otherwise remain unscrutinized. But it is incumbent on the Department to exercise its power carefully, accomplishing its mission in a manner that observes individual rights and protects the

[25] CBP Directive, *supra* note 3, at § 5.3.2.3; ICE Directive, *supra* note 3, at § 8.4(2).

[26] October 2010 Muster, *supra* note 2.

[27] CBP Directive, *supra* note 3, at §§ 5.4.2.2-5.4.2.3; ICE Directive, *supra* note 3, at §§ 8.5(2)(b)-(c). The October 2010 Muster reemphasizes the destruction requirement and clarifies that "destruction" refers to the deleting, shredding, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C. October 2010 Muster, *supra* note 2.

[28] CBP Directive, *supra* note 3, at § 5.3.2.6.

[29] CBP Directive, *supra* note 3, at § 5.3.1.3; U.S. Customs and Border Protection, Dep't of Homeland Sec., Inspection of Electronic Devices, 0204-0709 (2009), *available at* http://www.cbp.gov/linkhandler/cgov/travel/admissibility/msa_tearsheet.ctt/msa_tearsheet.pdf.

[30] CBP Directive, *supra* note 3, at § 5.3.1.4; ICE Directive, *supra* note 3, at §§ 8.2(1-4).

dignity of those whom we serve. Accordingly, in addition to evaluating the lawfulness of DHS policies governing the border search of electronic devices, we have evaluated a number of policy ideas, most directed at the Department in various forms by civil rights and immigration advocacy groups, to determine whether additional civil rights and civil liberties protections are necessary or useful. Our five recommendations have already been set out in the introduction to this Assessment, above, and are discussed below. Note, however, that as a result of our law and policy review, we reach the following conclusions about steps that we believe *need not* be taken:

- CBP and ICE need not institute a policy requirement of reasonable suspicion as a predicate for electronic device searches.
- CBP and ICE electronic border search policies do not violate travelers' First Amendment rights as defined by the courts.
- Additional time limits on electronic searching are not necessary; current policy ensures reasonable efforts at promptness.
- Additional safeguards are not needed with respect to privileged or sensitive information; current policy and training are sufficient.

The rationales underlying both our recommendations and our decision against particular recommendations are set forth in the following sections.

A. Authority to Search Electronic Devices at the Border

1. Fourth Amendment

Border Search Authority

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5) [redacted]

(b) (5) [redacted]

(b) (5) [redacted]

(b) (5) [redacted]. Indeed, both the CBP and ICE directives contain a number of rights protections beyond those that have been required by courts. In particular, as already mentioned, CBP and ICE policies require the following:

- Searches of electronic devices are conducted with the traveler's knowledge and presence, unless there are particular national security or law enforcement considerations that make it inappropriate to permit the individual to remain present.[34]

---

[33] CBP Directive, *supra* note 3, at § 5.3.2.2; ICE Directive, *supra* note 3, at § 8.4.

[34] CBP Directive, *supra* note 3, at § 5.1.4; ICE Directive, *supra* note 3, at § 8.1(2).

- Searches of electronic devices are documented in appropriate systems of records.[35]
- Retention of data is forbidden in the absence of probable cause to believe a crime has been committed, unless the retained data pertains to immigration, customs, or other enforcement matters. In any event, such retention must be consistent with the privacy and data protection standards of the system of records in which such information is being retained.[36]
- Data destruction requirements are specified and quite strict. If data is not being retained, CBP and ICE generally have seven days to destroy the data. A certified forensic agent with specialized expertise destroys any electronic evidence. If circumstances require additional time, supervisor approval is required to obtain an extension to no more than 21 days.[37]
- Data is safeguarded and stored[38] to comply with detailed reporting and management requirements.[39]
- Device detention periods are limited, unless an extension of time is approved. Subject to applicable extensions, CBP generally has up to five days to conduct the search of the electronic device while ICE has up to 30 days.[40]
- Supervisory oversight is emphasized. CBP requires supervisors to be present for electronic devices searches where practicable and requires supervisory approval to detain the device or image its memory so that the search might continue after the traveler departs from the port of entry.[41]
- Reasonable suspicion is required for searches that seek subject matter assistance from federal or non-federal agencies outside DHS.[42]

These polices address many of the civil rights and civil liberties concerns raised by the public and Congress about border examinations of electronic devices.

In sum, the overall authority to conduct border searches without suspicion or warrant is clear and long-standing, and courts have not treated searches of electronic devices any differently from searches of other objects. CRCL concludes that CBP's and ICE's current border search policies comply with the Fourth Amendment. We also recognize that the law regarding searches of electronic devices will continue to develop. Therefore, CRCL will continue to work with DHS

---

[35] CBP Directive, *supra* note 3, at § 5.1.3; U.S. Immigration and Customs Enforcement, Office of Investigations (OI) Guidance, Dep't of Homeland Sec., Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices (Dec. 12, 2008); ICE Directive, *supra* note 3, at § 8.2(1).

[36] CBP Directive, *supra* note 3, at § 5.4.1.2; ICE Directive, *supra* note 3, at § 8.5(1).

[37] CBP Directive, *supra* note 3, at §§ 5.3.1.2 & 5.4.1.2; ICE Directive, *supra* note 3, at § 8.5(e).

[38] CBP Directive, *supra* note 3, at § 5.4.1.5; ICE Directive, *supra* note 3, at § 8.5(1)(d).

[39] CBP Directive, *supra* note 3, at §§ 5.5 & 5.6.

[40] CBP Directive, *supra* note 3, at § 5.3.1; ICE Directive, *supra* note 3, at § 8.3(1).

[41] CBP Directive, *supra* note 3, at §§ 5.2-5.3.1.4. By contrast, ICE Special Agents are empowered to make investigative decisions based on the particular facts and circumstances of each case and do not require supervisory approval. ICE Directive, *supra* note 3, at § 6.1.

[42] CBP Directive, *supra* note 3, at § 5.3.2.2; ICE Directive, *supra* note 3, at § 8.4.

component agencies to ensure that civil rights and civil liberties are protected in this as in other areas.

2. *A Suspicion-Based Rule Is Not Advisable*

Notwithstanding the case law that suspicionless searching of electronic devices at the border is constitutionally permissible, some critics have advocated increased traveler protections as a matter of policy, in the form of a firm administrative standard requiring the presence of reasonable suspicion that a crime has been committed prior to any electronic device search. One specific model that has been suggested[43] as an alternative to the current ICE and CBP policies is a 1986 policy, Customs Directive 3340-006, *Review, Copying and Seizing of Documents* (June 12, 1986). We do not believe that this 1986 approach, or a reasonable suspicion requirement in any other form, would improve current policy.

At the outset, we note that CBP and ICE are charged with exercising far broader authorities at the border than was the former U.S. Customs Service. As renamed and reorganized in 2003, CBP enforces a broad range of customs, immigration, agriculture, and other federal laws at the border. Perhaps most importantly, CBP stands as the first line of defense in furtherance of the Department's national security and anti-terrorism responsibilities, articulated in the Homeland Security Act of 2002, as amended, 6 U.S.C. § 201 (2006), and elsewhere. Similarly, ICE, which received part of the former Customs Service, was created in 2003 to house all customs and immigration investigators, and is responsible for investigating all crimes relating to the border.

In addition, we note that although the 1986 policy directed that "Customs Officers should not read personal correspondence contained in travelers' baggage or on the person," it simultaneously authorized warrantless, suspicionless inspection procedures permitting extensive reading to allow officers to ascertain the content of the documents. Officers were directed to first read the document or paper by "scanning,"[44] in order to determine what action was appropriate."[45] Next, the officer was permitted, without suspicion or warrant, to fully read any documents that "appear[ed] to relate" to any one of the Customs Service's enforcement, regulatory or administrative functions listed within the policy. Then, if it was not "immediately apparent whether the document [was] admissible or subject to seizure," a document could be detained for a reasonable period of time upon reasonable suspicion that it belonged to a category of goods and subject to customs enforcement, regulation, or administration.[46] In short, like the current ICE and CBP policies, the 1986 policy allowed multiple warrantless, suspicionless readings of documents, in varying degrees of detail, to ensure compliance with applicable law.

---

[43] Ellen Nakashima, *Expanded Powers to Search Travelers at Border Detailed*, Washington Post, September 23, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/09/22/AR2008092202843 html.

[44] U.S. Customs Serv., Directive 3340-006, *Review, Copying and Seizing of Documents* (June 12, 1986), § 5(b) [hereinafter Directive 3340-006].

[45] Seditious materials were included among the types of documents that could be examined further. These were defined in the 1986 policy as materials "inciting or producing imminent lawless action, or prohibited matter being imported in violation of 19 U.S.C. § 1305." Directive 3340-006, *supra* note 44 at § 5(a)(v).

[46] Directive 3340-006, *supra* note 44 at § 5(e).

Whatever the parameters of the 1986 policy, adding a heightened threshold requirement could be operationally harmful without concomitant civil rights/civil liberties benefit. First, commonplace decisions to search electronic devices might be opened to litigation challenging the reasons for the search. In addition to interfering with a carefully constructed border security system, the litigation could directly undermine national security by requiring the government to produce sensitive investigative and national security information to justify some of the most critical searches. Even a policy change entirely unenforceable by courts might be problematic; we have been presented with some noteworthy CBP and ICE success stories based on hard-to-articulate intuitions or hunches based on officer experience and judgment. Under a reasonable suspicion requirement, officers might hesitate to search an individual's device without the presence of articulable factors capable of being formally defended, despite having an intuition or hunch based on experience that justified a search. Although this Office does not advocate arbitrary decision-making, we understand that there may be occasions where officers have only a few seconds to make important decisions about admissions and searches, and where they lack the opportunity to use routine criminal investigative techniques to develop reasonable suspicion or probable cause to justify the inspection of containers. Officers must therefore frequently make important choices based on inadequate and imperfect information. We note that officers very likely do have reasonable suspicion in most searches of electronic devices based on existing screening methods and objective factors; however, in light of the diminished expectations of privacy at the border and the government's paramount interest in border security, as well as the methods and objective factors ordinarily applied in making decisions, we conclude heightened suspicion requirements for searches of electronic devices at the border are not appropriate.

At the same time, the absence of information about *why* a particular search was performed renders supervision more difficult. The information could be used by supervisors or managers to understand whether the authority is being overused, in light of resources and priorities. Accordingly, our first recommendation is:

1. ***Rationale:*** **CBP officers who decide to conduct a device search generally should record the reason for the search in a TECS field. The reason should specifically relate to the decision to inspect an electronic device, not merely the selection for secondary screening (although the reason for both may be the same). To be clear, we are not recommending that officers demonstrate reasonable suspicion for the device search; rather we recommend that officers simply record the actual reason they are conducting the search, whatever that reason is. This recommendation exceeds constitutional requirements, but should facilitate CBP's operational supervision and oversight.**

B. First Amendment

(b) (5)

(b) (5)

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] The laptop border searches in the ICE and CBP policies do not violate travelers' First Amendment rights as defined by the courts.

C. Equal Protection and Religious/Ethnicity Discrimination

Civil rights and civil liberties advocacy groups have also raised concerns that particular religious and ethnic communities are being improperly singled out at the border for undue law enforcement attention in general and electronic media searches in particular.

Neither CBP nor ICE has an explicit written policy or training forbidding use of known or perceived religion as a screening criterion, although leadership within both Components has stated in less

formal ways that religious discrimination is unacceptable. With respect to race and ethnicity, there is extant written guidance. Pursuant to the Department of Justice's 2003 Guidance Regarding the Use of Race by Federal Law Enforcement Agencies[48] and DHS's 2004 Commitment to Race Neutrality in Law Enforcement Activities,[49] ICE and CBP personnel are permitted to use race or ethnicity as factors in a decision to search a person or object only based on information that is specific to an incident, suspect, or ongoing criminal activity, or as part of a narrowly tailored response to a compelling state interest involving national security or border integrity. During interviews, ICE and CBP personnel explained that officers are affirmatively taught not to rely on these constitutionally suspect classifications in searching electronic devices except based on information specific to particular suspects, incidents, or ongoing criminal activities, and that they are reminded regularly of the prohibition.

(b) (5)

[redacted] Our second recommendation would further consistency, and provide additional civil rights and civil liberties protection:

2. ***Antidiscrimination Policy:*** **CBP and ICE should state explicitly in policy that it is generally impermissible for officers to discriminate against travelers—including by singling them out for specially rigorous searching—because of their actual or perceived religion, and that officers may use race, religion, or ethnicity as a factor in conducting**

[48] Civil Rights Division, U.S. Dep't of Justice, Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (2003), *available at*: http://www.justice.gov/crt/about/spl/documents/guidance_on_race.pdf.

[49] U.S. Dep't of Homeland Sec., The Department of Homeland Security's Commitment to Race Neutrality in Law Enforcement Activities (2004), *available at:* http://www.dhs.gov/xlibrary/assets/CRCL_MemoCommitmentRaceNeutrality_June04.pdf.

(b) (5)

discretionary device searches only when (a) based on information (such as a suspect description) specific to an incident, suspect, or ongoing criminal activity, or (b) limited to situations in which Component leadership has found such consideration temporarily necessary based on their assessment of intelligence and risk, because alternatives do not meet border security needs.

Some advocacy organizations have also suggested that electronic device searching has very disproportionate effects on travelers whose ethnic or national background is Arab or Middle Eastern and that these effects are onerous and unjustified. To explore the factual premises that underlie this concern, CRCL and CBP have analyzed two years of data on electronic device searches. We have together concluded that if a port with a relatively high volume of device searches concentrates those searches among travelers within particular demographic groups, enhanced training and supervision can help to ensure that such concentration is not the result of bias or other inappropriate decision-making. Through the data analysis, CRCL and CBP have developed a framework for appropriate ongoing collection of statistical information to enable periodic review of this possibility. Our third and fourth recommendations are based on this analysis, and in accordance with this agreed-upon framework:

3. ***Regular Monitoring:*** **CBP should improve monitoring of the distribution of electronic device searching by race and ethnicity, by conducting routine analysis, including annual examination of electronic device searches by port of entry. After controlling for known relevant and permissible factors, such as port traveler demographics, and inclusion in watchlists, lookouts, and targeting rules, the analysis should assess whether travelers of any particular ethnicity—estimated using nationality/country of birth and name analysis—at any port of entry are being chosen for electronic device searches in substantial disproportion to that ethnicity's portion of all travelers through the port. The analysis should also consider U.S. citizens separately from others. Data and results should be shared with CRCL.**

4. ***Subsequent Supervision:*** **If it appears that electronic device searching in any port has a substantial unexplained skew towards travelers of one or more ethnicity, CBP should work with CRCL on developing appropriate oversight mechanisms. Subsequent steps generally should include a requirement of supervisory approval for searches (absent exigent circumstances) or enhanced training, and may include other responses.**

D. Time Limits

Some critics of electronic border searches have also suggested stringent time limits for completion of searches. Again, they point to the 1986 Customs policy as a model. But whereas the 1986 policy relied on a brief perusal of documents to determine if reasonable suspicion or probable cause existed, the continuous evolution and advancement of technology requires a more flexible approach for officers to evaluate electronic devices. The main difference between the 1986 policy and current policy is that under the current policy, if a border search of an electronic device requires more than a very brief period of time, officers are permitted, without articulating a reason for suspicion, to detain the device or copy its contents to complete the search. The 1986 policy envisioned an officer paging through the travelers' documents, looking them over quickly to determine if reasonable suspicion (or probable cause) was present, and reading them in more depth if circumstances warranted it. This

approach is not tenable in the context of modern electronic devices. Gigabytes of information may be stored in password-protected files, encrypted portions of hard drives, or in a manner intended to obscure information from observation. An on-the-spot perusal of electronic devices following the procedures established in 1986 could well result in a delay of days or weeks; even a cursory examination of the contents of a laptop might require a team of officers to spend days or weeks skimming the voluminous contents of the device. At the same time, a firm time limit for completing a search risks allowing a wrongdoer to "run out the clock" by encrypting and password-protecting his device, or traveling with voluminous amounts of documents, or other measures to make the search very time consuming.

The 2009 policies address the government's interest in enforcement of the laws and the traveler's interest in personal autonomy and convenience by permitting a broad search, while taking steps to decrease traveler inconvenience where the search is time-consuming. Although the time limits are somewhat flexible, it seems likely that the firm requirements for officers to seek and receive increasing levels of supervisory approval for extended detention push officers to ensure that detailed searches are completed as quickly as possible. Various computer-assisted search methods aim to balance comprehensiveness against timeliness. In light of the ever-increasing amounts of data stored on electronic devices and ever-more-complex storage and encryption methods, we believe ICE and CBP are making reasonable efforts to ensure border searches are completed as promptly as possible; no further policy change is recommended.

E. Privileged Materials

Some critics have suggested that officers should be prohibited from searching communications for which a traveler claims legal privileges, such as attorney-client privilege. Such a restriction would create an obvious safe harbor for the smugglers of child pornography, for terrorist conspirators, and any criminals relying on the transfer of information across borders. We note that the current policies safeguard sensitive material with procedural protections. The directives address attorney-client privileged materials and attorney work product by requiring an officer who suspects that the content of a traveler's privileged document may constitute evidence of a crime or otherwise pertains to a determination within ICE and CBP jurisdiction, to consult with ICE or CBP counsel.[51] For other types of sensitive information—business or commercial information, trade secrets, and medical records, for example—the directives state that officers should comply with applicable statutory provisions and regulatory guidelines, and should ask counsel for assistance if necessary.[52] This is fully covered in the mandatory training that all CBP officers take. None of the complaints currently pending before or known to CRCL present concerns related to the discovery or sharing of privileged material.[53] We conclude that current safeguards in these areas are sufficient.

---

[51] CBP Directive, *supra* note 3, at § 5.2.1; ICE Directive, *supra* note 3, at § 8.6(2)(b).

[52] CBP Directive, *supra* note 3, at § 5.4.2.2-5.4.2.3; Ice Directive, *supra* note 3, at § 8.5(2)(b)-(c).

[53] The plaintiff in *House v. Napolitano* asserts as a factual matter that materials seized from him were "privileged," *see* Complaint at 8, *House v. Napolitano*, but does not claim that the materials in question were protected by a recognized legal privilege.

F. Improved Notice about Redress

Following release of the August 2009 policies, CBP improved its airport signage and began providing a "tear sheet" to individuals whose electronic devices are searched. The airport signs better explain border search authority, provide Privacy Act information regarding electronic device searches, and explain the consequences for failure to provide information upon CBP questioning. The tear sheet explains to travelers whose devices are searched why they may have been selected, the legal authority for the device search, and what the traveler should expect from CBP.[54] The information provided about how to seek redress, however, is limited. The tear sheet includes contact information for the CBP info center, and it also states:

> The DHS Office for Civil Rights and Civil Liberties investigates complaints alleging a violation by DHS employees of an individual's civil rights or civil liberties. Additional information about the Office is available at www.dhs.gov/civilliberties.

More could be done to increase transparency and provide improved notice to travelers (at the very least, the form should provide the most up-to-date URL for CRCL's website: www.dhs.gov/crcl). At the same time, it is difficult to get all the relevant information on a short tear sheet. Our final recommendation is, therefore:

5. ***Improved Notice:* CBP should improve the notice given to travelers subjected to electronic device searches by updating tear sheets to refer travelers to DHS TRIP if they seek redress.**

We note in this regard that (at CRCL's request) TSA has recently updated DHS TRIP to give travelers a larger list of options from which to choose when seeking redress. Specifically, a traveler may now use the DHS TRIP system to complain that he/she was discriminated against on the basis of race, ethnicity, religion, disability, or gender; that he/she received questioning or treatment during screening that was abusive or coercive; and that a search of his/her person violated freedom of speech or press.

IV. Conclusion

Electronic device searching at the border is an important issue, presenting several potentially competing concerns. The traveling public is entitled to cross our borders without Fourth and First Amendment violations or invidious discrimination on the basis of race, ethnicity, religion, or other protected characteristic. The 2009 Directives guide CBP and ICE in lawfully fulfilling their responsibilities to safeguard against, for example, overly intrusive, discriminatory, and excessively time-consuming searches of electronic devices.

We conclude that, in accordance with established case law, officers may, as a matter of both constitutional law and sound policy, search electronic devices at the border without reasonable suspicion of wrongdoing. We further conclude that electronic device searches conducted in

[54] U.S. Customs and Border Protection, Dep't of Homeland Sec., Publication 0204-0709, Inspection of Electronic Devices, *available at*: http://www.cbp.gov/linkhandler/cgov/travel/admissibility/msa_tearsheet.ctt/msa_tearsheet.pdf.

accordance with the 2009 Directives do not violate travelers' First Amendment rights or the Equal Protection clause, contain reasonable (if flexible) time limits, and contain sufficient safeguards to protect privileged communications. However, we have offered several recommendations for improved oversight and communication about redress; we believe that these recommendations can augment civil rights protections without impeding operational requirements and effectiveness.

Margo Schlanger

Margo Schlanger
Officer for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
December 29, 2011

(b) (6) [redacted]

From: Kessler, Tamara
Sent: Wednesday, October 10, 2012 10:31 AM
To: (b) (6) [redacted]
Cc: Schlanger, Margo; (b) (6) [redacted]
Subject: Update on laptop Impact Assessment implementation and new data

Hi (b) (6) [redacted] As I believe you know, several of your staff have been working with mine to implement the recommendations of the CRCL Impact Assessment on border searches of electronic devices, which S1 signed off on last spring. The collaboration seems to be going very well, and we really appreciate the diligent work by OFO to update the traveler "tear sheet," improve the nondiscrimination policy presented in the officer training on device searches, and to improve record-keeping on device searches.

As you may also have heard, however, OFO re-reviewed a number of the TECS narratives from device searches at JFK and BOS, where we had been most concerned about disproportionate searches on travelers with Arab or Muslim names, and determined that the way the data had previously been coded for us failed to take into account a number of reasons why a referral to secondary inspection would be mandatory. In particular, it seems that a large number of records that appeared to us to be discretionary secondary inspections were, in fact, mandatory due to (b) (7)(E) [redacted]
(b) (7)(E) [redacted]

As a result, there turn out to be very, very few truly discretionary referrals that resulted in device searches at those ports during the two years for which we have data (FY2009-10). And so we cannot conclude that there is a problem at those airports that requires additional diversity training. We stand by the recommendation that this data analysis continue (and OFO has indicated it should have FY11-12 data for us to review by the end of the calendar year), and we stand by the recommendation that, *if* the data showed a problem at particular ports, there should be refresher training conducted at those ports. But we're withdrawing the proposed training materials you saw for JFK and BOS this year.

(b) (5) [redacted] Please let me know if you're satisfied with that approach.

Thanks. I hope you are well. Tamara

Tamara Kessler
Acting Officer
Office for Civil Rights & Civil Liberties
U.S. Department of Homeland Security
(b) (6) [redacted]

Homeland Security

~~For Official Use Only~~

Office for Civil Rights and Civil Liberties, Bi-Weekly Report
Thursday, October 11, 2012
Tamara Kessler

Border Search of Electronic Devices Impact Assessment

I have a set of updates on the CRCL Impact Assessment on border searches of electronic devices (laptops, cell phones, etc.), which you received in final form last spring. Since then CRCL and CBP OFO have been working on implementation of our recommendations. CBP is printing updated "tear sheets" for persons who receive a device search, which will include language referring them to DHS-TRIP; CBP has updated its training and policy to reflect our recommendations stressing non-discrimination on the basis of religion; and a new CBP system is permitting fuller narratives to be recorded of secondary inspections that include a device search.

However – in working closely with CBP on this project, CBP had occasion to re-examine the way some of the TECS records were coded for our statistical review, and it turns out that a very large number of records had not been appropriately coded to reflect the fact that the secondary inspection was, effectively, (b)(7)(E) [redacted] So our conclusions about the racial/ethnic impact of device searches, and in particular our concern that at two large airports the discretionary searches were falling disproportionately on Arab and Muslim travelers, are no longer well-founded. That is, there were *so few* device searches following a truly discretionary referral of an individual from primary to secondary inspection that we can't infer any behavior by front-line OFO officers that might have been prompted by the ethnicity of travelers.

This new conclusion from the data does *not* affect our recommendations to CBP. It does mean, however, that based on the FY 2009-2010 data we have reviewed so far, there are not any ports where additional diversity training should be required on this basis. CBP expects to provide us data from device searches conducted in FY 2011 and FY 2012 by the end of calendar year 2012, at which time we will analyze that data to see if there appears to be any notable ethnic disproportion in the distribution of discretionary (i.e., non-intelligence-driven) device searches.

Non-Responsive to the Request [redacted]

Office for Civil Rights and Civil Liberties, Bi-Weekly Report
Thursday, October 11, 2012
Tamara Kessler

Non-Responsive to the Request

[redacted]

Non-Responsive to the Request

[redacted]

Non-Responsive to the Request

[redacted]

[redacted]

Non-Responsive to the Request

[redacted]

POLICIES CURRENTLY IN PLACE THAT SAFEGUARD CIVIL RIGHTS AND CIVIL LIBERTIES DURING SEARCHES OF ELECTRONIC DEVICES AT THE BORDER:

- Searches of electronic devices are conducted with the traveler's knowledge and presence, unless there are national security or law enforcement considerations that make it inappropriate to permit the individual to remain present.
- Searches of electronic devices are documented in appropriate systems of records.
- Retention of data is forbidden in the absence of probable cause to believe a crime has been committed, unless the retained data pertains to immigration, Customs, or other enforcement matters. In any event, such retention must be consistent with the privacy and data protection standards of the system of records in which such information is being retained.
- Data destruction requirements are specified and quite strict. If data is not being retained, CBP and ICE generally have seven days to destroy the data. A certified forensic agent with specialized expertise destroys any electronic evidence. If circumstances require additional time, supervisor approval is required to obtain an extension to no more than 21 days.
- Data is safeguarded and stored to comply with detailed reporting and management requirements.
- Device detention periods are limited, unless an extension of time is approved. Subject to applicable extensions, CBP generally has up to five days to conduct the search of the electronic device while ICE has up to 30 days.
- Supervisory oversight is emphasized. CBP requires supervisors to be present for electronic device searches where practicable and requires supervisory approval to detain the device or image its memory so that the search might continue after the traveler departs from the port of entry.
- Reasonable suspicion is required for searches that seek subject matter assistance from Federal or non-Federal agencies outside DHS.

THE CONSTITUTION PROJECT

Safeguarding Liberty, Justice & the Rule of Law

Suspicionless Border Searches of Electronic Devices:

Legal and Privacy Concerns with The Department of Homeland Security's Policy

A REPORT BY THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY COMMITTEE

May 18, 2011

The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036
(202) 580-6920 (tel)
(202) 580-6929 (fax)
info@constitutionproject.org

www.constitutionproject.org

Suspicionless Border Searches of Electronic Devices:
Legal and Privacy Concerns with The Department of Homeland Security's Policy

---

The Fourth Amendment to the Constitution establishes the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and dictates that a warrant must be substantiated by probable cause.[1] There are few exceptions to this constitutional requirement for a warrant. One is for searches at the border or the functional equivalent of the border, where routine searches without probable cause have been permitted.[2] Relying on this longstanding exception to the Fourth Amendment's warrant requirement, federal statutes authorize customs and immigration officials to routinely search packages, baggage, merchandise, and even travelers themselves as they cross the border into the United States.[3] Such border searches can be conducted pursuant to these statutes without a warrant, without probable cause, and without suspicion of wrongdoing. However, these searches increasingly have been expanded beyond the original intent of the border search exception to intercept contraband, and are now used to capture volumes of private and personal information carried across the border in computers and other electronic devices.

The authority claimed by customs officials to search the belongings of travelers extends to any item a traveler may carry, including electronic devices.[4] For some time customs and immigration officers have relied upon the border search exception to the Fourth Amendment to search, review, copy, and detain various types of electronic devices, including laptop computers, computer disks, cell phones, electronic tablets, portable storage devices, and other electronic media, all without first obtaining a warrant or even without having reasonable suspicion of wrongdoing. These searches are conducted by both Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). Between October 1, 2008 and June 2, 2010, over 6,500 people – almost half of whom were U.S. citizens – were subjected to searches of their electronic devices upon crossing the international border.[5] Of course, given the volume of information that these devices typically carry – some of which the traveler may not be aware of – the potential for intrusion into a person's privacy far exceeds that relating to the search of non-electronic items.

---

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

[2] See *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) ("Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant . . . ."); *United States v. Ramsey*, 431 U.S. 606, 619 (1977) (the "longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself").

[3] See, e.g., 19 U.S.C. § 1496 (providing that the "appropriate customs officer may cause an examination to be made of the baggage of any person arriving in the United States"), and 19 C.F.R. § 162.6 ("All persons, baggage, and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs officer.").

[4] See *United States v. Arnold*, 523 F.3d 941, 946 (9th Cir. 2008) ("we are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage device at the border").

[5] Analysis of documents released pursuant to Freedom of Information Act, available at: http://www.aclu.org/national-security/government-data-about-searches-international-travelers-laptops-and-personal-electr

Historically, the scope of what was covered by the border search exception was fairly limited, since the exception is confined to the items a traveler carries across the border. As a practical matter, most private documents, letters, photographs, and other personal effects would remain in an individual's home, safeguarded by full Fourth Amendment protections and the warrant requirement. With today's technology, however, people can and do travel with vast quantities of private, personal information stored on their laptops and other electronic devices. Unlike at any time in the past, individuals who travel internationally, by virtue of legitimately choosing to carry electronic devices, are unknowingly subjecting volumes of personal information to involuntary and suspicionless search and review by federal law enforcement authorities. This problem is compounded by the fact that many electronic devices are used to carry both personal and business-related information. The continual evolution in how people use electronic devices in their everyday lives creates growing tension between the Fourth Amendment guarantees and what historically has been viewed as a narrow exception to the requirements for probable cause and a warrant.

In August 2009 CBP and ICE issued Directives that formalized their 2008 policy governing how their officers conduct searches of these devices. These Directives raise several serious constitutional concerns, however. First, the Directives, by permitting searches to be carried out without reasonable suspicion of wrongdoing long after the traveler has crossed the border, may contravene well-established Fourth Amendment principles. Second, the Directives allow for searches that are far more intrusive than the ordinary border searches that historically have occurred, and can have a chilling effect on free speech, as information created or stored on an electronic device is subject to search simply by virtue of being carried across the border. The Directives also can open avenues for other constitutional abuses, such as racial or religious profiling or circumventing Fourth Amendment requirements that, in other contexts, would mandate issuance of a warrant prior to a search. Similarly, even when officers do possess reasonable suspicion, the lack of proper safeguards and guidelines as to the scope of permitted searches allows law enforcement officials to engage in wide-ranging searches of devices and information that have no connection to the underlying predicate for the search.

For these reasons and as outlined further below, we, the undersigned members of the Constitution Project's bipartisan Liberty and Security Committee, urge the Department of Homeland Security (DHS) to discontinue its policy of searching electronic devices at the border without reasonable suspicion. We further recommend that DHS amend the CBP and ICE Directives on Border Searches of Electronic Devices to explicitly require reasonable suspicion of wrongdoing before allowing searches of electronic devices at the border; in the case of U.S. persons, to require a probable cause warrant before law enforcement may retain copies of data retrieved from an electronic device and before they may search electronic devices or their contents for a period longer than is needed for a reasonable search (presumptively a maximum of 24 hours); and to establish safeguards prohibiting racial or religious profiling and, in the case of U.S. persons, requiring that the scope of a search be tied to the underlying predicate for the search, so that a search does not turn into a "fishing expedition" or become unnecessarily intrusive.[6]

In developing these recommendations, the Committee considered whether the standards for border searches of electronic devices should differ depending on the nationality of the person

[6] We are also troubled by intrusive physical searches at the border, but such practices are beyond the scope of this report.

searched. The U.S. Supreme Court has not fully clarified the extent to which Fourth Amendment protections apply to non-citizens outside the United States (or at the border crossing). Although some committee members take the position that the reasonable suspicion and probable cause standards this report recommends for U.S. persons should apply equally to non-U.S. persons, the Committee agreed on the recommendations outlined below which make some distinctions in the case of non-U.S. persons as a significant improvement to the status quo.[7] Further, committee members agree that as discussed in further detail below, *suspicionless* searches of electronic devices at the border are an inefficient law enforcement technique for detecting and preventing national security threats, and reasonable suspicion of illegality should be required to justify any such searches.

I. CBP AND ICE BORDER SEARCHES OF ELECTRONIC DEVICES

A. The CBP and ICE Directives

In August 2009, Customs and Border Protection and Immigration and Customs Enforcement each announced their respective Directives setting forth the policies and procedures governing border searches of electronic devices.[8] Both Directives detail the circumstances in which CBP and ICE officials may search, detain, and seize electronic devices and set standards for the handling of any information collected. Most significantly, both Directives allow for searches of electronic devices absent individualized suspicion. CBP and ICE officers may detain an electronic device, without reasonable suspicion, for a "reasonable" period of time to conduct searches and to receive technical assistance (e.g., translation or decryption) in searching the device. Searches can take place on or off the port of entry facility and can be done outside the presence of the owner.

Despite their common approaches, there are material differences between the two Directives that can affect travelers' interests in their electronic devices. For example, CBP officers must obtain supervisory approval to detain a device once the traveler has left the port of entry. ICE officers do not need similar approvals.[9] Also, the amount of time that CBP and ICE can detain a device can differ significantly. The CBP Directive states that detentions should not exceed five days, and while extensions can be granted by certain supervisors, extensions beyond 15 days can be granted only in seven-day increments. The ICE Directive, in contrast, states only that detentions should be completed within a "reasonable time." What constitutes a reasonable time under the Directive depends on several factors: the volume of information reviewed, whether the traveler continued on his or her journey without the device, whether technical or subject matter assistance was sought, whether ICE attempted to ensure timely receipt of assistance, whether the traveler took affirmative and timely steps to prevent the search of the device, and

---

[7] A "United States person" is defined by statute as "a citizen of the United States" and "an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8)." 50 U.S.C. § 1801(i). We use the term "U.S. person" to cover both groups together.

[8] The CBP and ICE Directives are available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf .

[9] The Privacy Impact Assessment that accompanied the Directives explained that ICE Special Agents do not need supervisory approval to detain a device because they are "federal criminal investigators," and that the "decision to detain or seize electronic devices or detain, seize, or copy information therefrom is a typical decision a Special Agent makes as part of his or her basic law enforcement duties." Department of Homeland Security, Privacy Impact Assessment for the Border Search of Electronic Devices, at 8 (Aug. 25, 2009) (hereinafter, "PIA").

any exigencies that might have arisen. Ultimately, the ICE Directive states that searches generally should be completed within 30 days, and any extensions must be approved by a supervisor every 15 days. In other words, if ICE detains a computer, it can keep it as long as 30 days without any supervisory approvals whereas CBP needs approvals after five days. Because ICE has "concurrent border search authority with CBP and may join or independently perform a boarder search at any time," the length of time someone may be deprived of his or her property can turn on whether CBP or ICE detains the device. Either way, neither Directive sets an absolute limit on how long the agencies can detain a device, and both allow immigration and customs officers to detain and search an electronic device without reasonable suspicion for a material length of time after the device first crossed the border.

B. CBP and ICE Border Search Practices

The CBP and ICE practice of searching electronic devices at the border without reasonable suspicion began several years ago. Even before the Directives were announced, it was the policy of customs and immigrations officials to allow searches of electronic devices without suspicion of wrongdoing.[10] This policy was used to search a variety of media, including laptop computers, cell phones, memory cards, digital cameras, thumb drives, compact disks, SIM cards, and hard drives.[11] In fact, in the first eight months of fiscal year 2009, CBP alone conducted 2,204 searches of electronic media under the policy in existence at that time, including laptops, resulting in 105 detentions (for which no reasonable suspicion was required) and 115 seizures.[12] These searches are far more intrusive than the important practice of requiring travelers to open and turn on electronic devices to demonstrate that the devices themselves are not actually bombs or other weapons.

Suspicionless border searches of the *content* of information stored on such devices are not justified by safety concerns and have proven invasive.

A 2008 letter from Congressman Bennie Thompson to CBP Commissioner Ralph Basham described CBP and ICE border search practices that extend far beyond searches for concealed contraband, weapons, or explosives:

> These practices include opening individual laptops; reading documents saved on the devices; accessing email accounts and reading through emails that have been sent and received; examining photographs; looking through personal calendars; and going through telephone numbers saved in cellular phones. Further, individuals have raised claims that these searches can sometimes last for hours and cause significant delay, while the

[10] See, e.g., Memorandum from Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection, to Directors, Field Operations, Director, Pre-Clearance, Office of Field Operations regarding New Policy Regarding Boarder Search/Examination of Documents, Papers, and Electronic Devices (July 18, 2008).

[11] See, Department of Homeland Security, Customs and Border Protection Field Operations Program Analysis and Measures Weekly Electronic Media Report. See also PIA at 6 ("This border search may include examination of documents, books, pamphlets, and other printed material, as well as computers, storage disks, hard dives, phones, personal digital assistants (PDAs), cameras, and other electronic devices.").

[12] *Id.*

> subject of the search – often a U.S. citizen – is delayed entering the country and must sit by as the information contained in their personal devices are copied, confiscated or compromised.[13]

Department of Homeland Security documents made public through a Freedom of Information Act lawsuit further highlight the practical effects of this policy.[14] In one instance, a traveler had a laptop computer and flash drive confiscated by CBP, and over six months later, he was still trying – with the help of his congressman – to secure the return of his possessions. Another traveler reported the search of a laptop despite putting CBP on notice that the computer contained confidential business information. On another occasion, a traveler had his laptop detained for more than a month, requiring him to buy a replacement for his job. And yet another traveler agreed to a search of several devices in an effort to avoid further delays. Reports prepared by the Asian Law Caucus and Muslim Advocates detail numerous examples in which U.S. persons have had to endure intrusive, suspicionless searches at the border.[15]

II. LEGAL AND POLICY CONCERNS WITH THE CBP AND ICE DIRECTIVES

A policy that allows customs and immigration officials to conduct suspicionless and broad-ranging searches of electronic devices raises significant constitutional concerns. As noted above, the nature of electronic devices is such that searches of these items are particularly more intrusive than searches of other baggage a traveler might carry – e.g., a briefcase or even paper documents – and are likely to intrude upon reasonable expectations of privacy. Even more troubling, by allowing CBP and ICE to detain electronic devices for days or months at a time and to remove the device from the port of entry for further searching, all without reasonable suspicion, the Directives conflict with the Fourth Amendment's basic requirements that searches and seizures be conducted reasonably and pursuant to a warrant based on probable cause.

A. The Directives Unreasonably Allow Suspicionless Searches Long After the Initial Border Crossing

As they currently exist, the Directives grant CBP and ICE officials overbroad authority to conduct suspicionless searches of electronic devices that may contravene Fourth Amendment standards. Such unreasonable searches can happen under the CBP and ICE Directives in at least two ways. First, CBP and ICE officers may detain electronic devices for significant periods of time. For CBP, detentions can be extended well beyond the minimum five-day guideline with supervisory approval. If the device is detained by ICE, the detention can last for "a reasonable time," which according to its Directive can last 30 days or more. In fact, under ICE's Directive, what is considered reasonable depends in part on the volume of data to be searched, which suggests that the more information there is to search, the longer ICE can "reasonably" detain the device. And neither Directive limits the total time a device may be detained. Second,

---

[13] Letter from The Honorable Bennie G. Thompson, Chairman, U.S. House of Representatives, Committee on Homeland Security, to The Honorable W. Ralph Basham, Commissioner, U.S. Customs and Border Protection, at 1 (July 1, 2008).

[14] These documents are available at: http://www.aclu.org/national-security/government-data-about-searches-international-travelers-laptops-and-personal-electr .

[15] See www.asianlawcaucus.org/wp-content/uploads/2009/04/Returning%20Home.pdf and www.muslimadvocates.org/documents/Unreasonable_Intrusions_2009.pdf .

detained devices can be searched at locations away from the port of entry. This is likely to happen if technical assistance is sought (i.e., decryption or translation is needed). There are no guidelines on where those off-site facilities may be located or whether the device might be sent to another law enforcement agency. Under any of these scenarios, the Directives allow searches to be conducted without any sort of suspicion as a predicate.

Fourth Amendment jurisprudence, however, recognizes that searches conducted at a time and place remote from the border "entail a greater intrusion on legitimate expectations of privacy."[16] Thus, at least some federal courts have required reasonable suspicion to support warrantless searches of electronic devices that otherwise would be permitted by the Directives. For instance:

- In a Michigan case from May 2010,[17] the government was required to establish reasonable suspicion to support the warrantless search of a laptop computer 20 miles away from and within 24 hours after the computer crossed the border.

- In a California case from June 2010,[18] the court ruled that a search of a laptop conducted at an off-site laboratory over two weeks after it was initially detained at an airport required reasonable suspicion.

To the extent, therefore, that the CBP and ICE Directives permit the detention of electronic devices without reasonable suspicion at a location removed from the actual border or its functional equivalent and at a time remote from the original border crossing, the Directives may impermissibly invade expectations of privacy and contravene well-settled Fourth Amendment principles.

B. The Directives Can Lead to Other Violations of Constitutional Rights

In addition to violating reasonable expectations of privacy, suspicionless border searches of electronic devices can lead to compromises of an individual's constitutional rights. First, the absence of any requisite level of suspicion to conduct border searches opens the doors to racial or religious profiling. Public accounts detail how this policy could be used to harass U.S. persons based on their racial, ethnic, or religious background.[19] A 2008 Congressional Research Service report came to the same conclusion: "If a customs official could conduct a search without providing cause, it would be difficult to deter ethnic profiling because the official would not need to explain why he conducted the search."[20] Law enforcement should focus on behaviors, and race, ethnicity, and religious affiliation should not be considered as factors that create suspicion unless these factors are used as part of a specific suspect description.

---

[16] *Niver*, 689 F.2d at 526. But see *United States v. Cotterman*, No. 09-10139 (9th Cir. Mar. 30, 2011) (upholding the suspicionless search of a laptop 170 miles from the border and four days after the device was detained at the border).

[17] *United States v. Stewart*, 2010 WL 2089355 at *4 (E.D. Mich. May 24, 2010).

[18] *United States v. Hanson*, Case 3:09-cr-00946 at 5-7 (N.D. Cal. June 2, 2010).

[19] See, e.g., Ellen Nakashima, The Washington Post, *Expanded Powers to Search Travelers at Border Detailed*, at A02 (Sept. 23, 2008).

[20] Yule Kim, *Border Searches of Laptops and Other Electronic Storage Devices*, Cong. Research Serv., at 8 (Mar. 5, 2008).

Second, and on a related note, the Directives' policy can be used by other law enforcement agencies as an end-run around the general warrant requirement to access information on a traveler's electronic devices. The potential for this abuse has reportedly already taken root. According to public reports, there has been discussion among various law enforcement agencies concerning the fact that CBP and ICE have the ability to search and detain information at the border that other law enforcement officials could not access without a warrant or at least further substantiation of wrongdoing.[21]

Third, a policy that allows customs and immigration agents to search electronic devices at will can burden free speech. The American Anthropological Association complained to DHS that such warrantless searches "not only violate the rights of the scholar, but they unlawfully infringe upon the lives of . . . research participants."[22] Likewise, at least one firm has warned its employees about DHS's policy, noting that "[t]here are no published guidelines as to what might trigger these searches," and warning employees who travel internationally to "take extra precaution with [the company's] proprietary information."[23] The burden that the Directives place on free speech rights has led to a recent lawsuit by the National Association of Criminal Defense Lawyers and the National Press Photographers Association.[24]

Finally, the scope and extent of searches of electronic devices have the potential to invade privacy on a level not possible with books, papers, or other non-electronic materials, a reality that even DHS itself recognizes.[25] Digital cameras can store hundreds of personal pictures. Computers not only store millions of pages worth of information, but also information on web sites visited. This can include cookies and other metadata that the individual does not even know exists on his or her computer and can cover a period of several years.

C. Further Safeguards are Needed to Ensure Constitutional Protections Even if There is Reasonable Suspicion of Wrongdoing

The Directives also lack adequate safeguards ensuring that a person's constitutional interests are protected once a search has begun. The Directives allow CBP and ICE officials to search any and all electronic devices that a traveler carries – including all of the information contained on those devices – regardless of whether there is reason to suspect the traveler of criminal wrongdoing or to suspect that the devices or the information they contain have any connection to a potential violation of the law.

---

[21] Ellen Nakashima, The Washington Post, *Expanded Powers to Search Travelers at Border Detailed*, at A02 (Sept. 23, 2008).

[22] Letter from Setha Low, President, American Anthropological Association, to The Honorable Michael Chertoff, Secretary, Department of Homeland Security (July 25, 2008), available at: http://www.aaanet.org/issues/AAA-Letter-on-Homeland-Security-Searches.cfm

[23] See Letter from The Honorable Dennis Moore, U.S. House of Representatives, to Transportation and Security Administration (May 13, 2008), available at: http://www.aclu.org/national-security/government-data-about-searches-international-travelers-laptops-and-personal-electr, pp. 000781-782.

[24] *Abidor v. Napolitano*, Case No.: CV10-4059 (E.D.N.Y. Sept. 7, 2010).

[25] See PIA at 2 ("Where someone may not feel that the inspection of a briefcase would raise significant privacy concerns because the volume of information to be searched is not great, that same person may feel that a search of their laptop increases the possibility of privacy risks due to the vast amount of information potentially available on electronic devices.").

The Fourth Amendment prohibition of unreasonable searches and seizures mandates the implementation of safeguards against free-ranging and open-ended searches, even for cases in which there was reasonable suspicion supporting the initial search. Such safeguards would be consistent with the Fourth Amendment's particularity requirement for warrants. Courts have insisted, especially when computers are the subject of searches, that warrants describe with particularity the scope of the search, and that officers executing the warrant not stray from those parameters.[26]

The authority to search a traveler's belongings at the border without a warrant or probable cause is an exception to the Fourth Amendment's requirements, and as such, it should be exercised narrowly and with clearly-defined limits.[27] Consequently, in the case of U.S. persons entitled to full Fourth Amendment protections, in addition to requiring reasonable suspicion of wrongdoing to initiate a border search of electronic devices, the Directives should also require that any such search be limited to those devices, files, and information that are likely to contain contraband or evidence of the unlawful activity that established the reasonable suspicion to search in the first instance. Such requirements would be consistent with how courts treat other exceptions to the warrant requirement.[28]

Thus, for U.S. persons, even when law enforcement officers have reasonable suspicion justifying a search, the scope and nature of the search should be based upon that reasonable suspicion, and should not include a "fishing expedition" or be more intrusive than necessary. The Fourth Amendment requires that even for search warrants predicated on a showing of probable cause, the warrant must "particularly" describe the place to be searched and the items to be seized. Searches of digital devices must similarly be circumscribed and tied to the predicate justifying the search.

The Directives also allow CBP and ICE to seek subject matter assistance from experts or other law enforcement agencies based solely on reasonable suspicion of wrongdoing. Subject matter assistance is defined in the Directives as assistance by other law enforcement agencies to "determine the meaning, context, or value of information contained therein as it relates to the laws enforced and administered" by CBP and ICE.[29] Because subject matter assistance involves other law enforcement agencies, the Directives contemplate even longer detention and search times than when no subject matter assistance is required. The CBP Directive, for instance, allows 15 days (as opposed to five days when subject matter assistance is not sought), with unlimited seven-day extensions, for the assisting agency to respond. The ICE Directive again allows "a reasonable period of time" for a response from the assisting agency and states only that ICE should "get a status report" sometime within the first 30 days.

---

[26] See, e.g., *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (suggesting methods to avoid searching files of the type not identified in the warrant, such as "observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory").

[27] See *Flippo v. West Virginia*, 528 U.S. 11, at 13 (1999) ("A warrantless search by the police is invalid unless it falls within one of the narrow and well-defined exceptions to the warrant requirements.") (emphasis added).

[28] See, e.g., *Maryland v. Buie*, 494 U.S. 325, at 335 (1990) ("A protective sweep is without question a 'search,' . . . they are permissible on less than probable cause only because they are limited to that which is necessary to protect the safety of officers and others."); *Flippo*, 528 U.S. at 13-15 (police needed a warrant to search the contents of a briefcase found at a crime scene).

[29] CBP Directive at 5.3.2.3. See also ICE Directive at 8.4(2)(a).

In order to continue searching the electronic device of a U.S. person for such lengthy time periods or to seize and retain copies of data stored on a device, the government must have a proper constitutional predicate beyond reasonable suspicion.[30] To be consistent with Fourth Amendment principles and the Directives themselves,[31] probable cause of wrongdoing should be required before officials may continue the search of an electronic device beyond the initial time period justified by reasonable suspicion. In this regard, we note that a Travelers' Privacy Protection Act bill introduced in the Senate two years ago would require probable cause for searches lasting over 24 hours. We agree that 24 hours may be an appropriate guideline, but this time limit should be based on what is actually reasonable under the circumstances, including how remote the border check point is and the level of law enforcement expertise that is readily available on site to conduct the search. Second, we recommend that a probable cause warrant should be required before officials may copy and retain data that is stored on an electronic device. If, however, officials believe the data may have intelligence value related to international terrorism and wish to seek a FISA search warrant, more time may be needed to complete that process. Thus, if officials have begun the application process to seek a FISA warrant during the 24 hour period described above, they should be permitted to retain the device for up to seven days if such additional time is needed to obtain a FISA warrant.

Thus, when officials begin a search based upon reasonable suspicion, they should use that period, presumptively up to 24 hours, to determine whether there is probable cause to justify detaining the device for longer than 24 hours and/or to retain copies of data found on the device. Assuming there was reasonable suspicion to justify the preliminary search, this search could permissibly include checking the device's data against watch lists, checking phone numbers and email addresses for contacts with known criminal or terrorist suspects, and seeking a FISA warrant, a national security letter (NSL) and/or a Patriot Act Section 215 order if any of these are appropriate under the circumstances. Law enforcement would only be permitted to detain the device beyond the preliminary search period (presumptively up to 24 hours) or to retain copies of the data, if this preliminary search leads them to develop probable cause, or if they are able to do so under one of these other authorities (FISA, Patriot Act, etc.). The permissible time period could be extended to up to seven days if officials need that time to seek a FISA warrant.

Even if probable cause is *not* established, any electronic trail created by the cross-checking of information against government watch lists and other databases should *not* be expunged, but should remain available for subsequent audits and oversight reviews. Officials should be prohibited, however, from putting the data into an intelligence system or database where the information is searchable or retrievable or can otherwise be mined by intelligence or law enforcement agents.

---

[30] See *Soldal v. Cook County, Illinois*, 506 U.S. 56, 61 (1992) ("A seizure of property, we have explained, occurs when there is some meaningful interference with an individual's possessory interests in that property.") (internal quotations omitted); *United States v. Place*, 462 U.S. 696, 708-710 (1983) (detention on less than probable cause of a traveler's luggage for 90 minutes was ruled an unreasonable seizure under the Fourth Amendment).

[31] Both the CBP and ICE Directives require probable cause to seize electronic devices. See CBP Directive at 5.4.1.1. and ICE Directive at 8.5(1)(a). Neither Directive attempts to define a "seizure," though from the context, the Directives appear to view a seizure as the indefinite retention of the device or its contents for law enforcement purposes.

D. Searches Based Upon Reasonable Suspicion will More Effectively Serve Law Enforcement Goals

Amending the Directives to require immigration and custom officials to have reasonable suspicion before conducting warrantless border searches of electronic devices would not diminish CBP's or ICE's law enforcement effectiveness. Reasonable suspicion is not a demanding standard. While there is no precise definition of what constitutes reasonable suspicion, it has been described as "a particularized and objective basis for suspecting the person stopped of criminal activity."[32] Thus, in a 2005 case decided by the Fourth Circuit Court of Appeals, the court found that customs officials had reasonable suspicion to search a laptop computer when they found drug paraphernalia, photos of child pornography, a disturbing video focused on a young boy, and an outstanding arrest warrant in the defendant's van.[33] In another case, reasonable suspicion to search a computer was established when the defendant's name was matched against a database of outstanding warrants for child pornography and officers found an unusual amount of computer equipment contained in the defendant's vehicle.[34] In fact, the CBP Directive states that "the presence of an individual on a government-operated and government-vetted terrorist watch list will be sufficient to create reasonable suspicion."[35]

Moreover, requiring reasonable suspicion to conduct a search of electronic devices would focus limited law enforcement resources where they can be most effective. Suspicionless searches are not well-suited to identifying and locating contraband or illegal material, as the CBP's own data show. In 2009, for example, only about 5% of the electronic devices searched at the border were seized as a result of the search. Put differently, in the vast majority of instances involving border searches of electronic devices, the traveler has had to needlessly withstand a significant intrusion into his or her privacy for no legitimate law enforcement purpose.

The overwhelming reality is that in the usual instance in which immigration and customs officials have uncovered illegal material being transported into the country using an electronic device, there has been independent, reasonable suspicion to search the device. Though courts routinely uphold the legality of assertedly suspicionless border searches of electronic devices, in virtually every case to consider the issue, the court also found facts supporting reasonable suspicion to conduct the searches.[36] This is supported by testimony from former-Secretary

---

[32] *Ornelas v. United States*, 517 U.S. 690, 696 (1996); see also *United States v. Arvizu*, 534 U.S. 266, 273 (2002) (reasonable suspicion is "a particularized and objective basis for suspecting legal wrongdoing").

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

[34] *United States v. McAuley*, 563 F. Supp.2d 672 (W.D. Tex. 2008).

[35] CBP Directive at 5.3.2.3. If the government establishes that reasonable suspicion is required before placing an individual's name on a watch list, this would be an appropriate, if circular, standard. However, under present watch list practices, it appears that far less than reasonable suspicion is required for watch listing, and if this is true, then this Directive should be amended to delete this statement. See, Ellen Nakashima, The Washington Post, *Terrorist Watch List: One Tip Now Enough to Put Name in Database, Officials Say* (Dec. 29, 2010).

[36] See *United States v. Romm*, 455 F.3d 990, 994 n.4 (9th Cir. 2006) (prior to the search officials discovered that defendant had pleaded nolo contendere to two counts of promoting sexual performance by a child and one count of child exploitation by means of a computer); *Ickes*, 393 F.3d at 507 ("The agents did not inspect the contents of Icke's computer until they had already discovered marijuana

Michael Chertoff to a congressional committee that in practice, border searches of electronic devices are done only when there is reasonable suspicion of wrongdoing.[37]

Recognizing that DHS's policy of suspicionless border searches of electronic devices not only intrudes on the rights of U.S. persons but does little to advance the law enforcement needs of DHS, several different legislative proposals have been made that would require reasonable suspicion before such searches could be performed. For instance, in 2008, Senator Feingold introduced the "Travelers' Privacy Protection Act of 2008," and in 2009, Congressman Engel proposed the "Securing Our Borders and Our Data Act of 2009." Both bills would require immigration and customs officials to have reasonable suspicion of wrongdoing before detaining and searching the contents of electronic devices and to obtain a warrant based on probable cause before seizing electronic devices.[38]

RECOMMENDATIONS FOR REFORM

For these reasons, we, the undersigned members of the Constitution Project's Liberty and Security Committee recommend that the Department of Homeland Security implement the following reforms:

1. Amend the CBP and ICE Directives to require that CBP and ICE officials may not search the content or information contained in electronic devices of U.S. persons unless there exists a reasonable suspicion that the electronic device contains illegal material or evidence of illegal conduct. In the case of non-U.S. persons, officials must have reasonable suspicion that the non-U.S. person is or was engaged in some illegal activity to support such a search. However, officials should still be permitted to conduct limited suspicionless searches aimed at verifying that a device is functioning and is not or does not contain a bomb or weapons. The definition of "electronic device" should include laptop computers, personal digital assistants,

---

paraphernalia, photo albums of child pornography, a disturbing video focused on a young boy, and an outstanding warrant for Ickes's arrest."); *United States v. Roberts*, 274 F.2d 1007, 1017 (5th Cir. 2001) (customs agents received information that defendant was about to board an international flight while carrying child pornography); *United States v. Hanson*, Case No. CR 09-00946, at 5 (N.D. Cal. June 2, 2010) ("the Court concludes that the Government has met its burden to show the February search was supported by reasonable suspicion"); *United States v. Stewart*, 2010 WL 2089355, at *4 (E.D. Mich. May 24, 2010) ("The Court believes instead that the ICE agents had reasonable suspicion to believe that the computers . . . contained contraband . . . .") *McAuley*, 563 F. Supp.2d at 678 n.7 ("the name check information coupled with the presence and amount of computer equipment the Defendant had is arguably sufficient information to determine the existence of reasonable suspicion"); *United States v. Bunty*, 617 F. Supp.2d 359, 364 (E.D. Pa. 2008) ("Even if reasonable suspicion were necessary, the Court is satisfied that the circumstances in this case give rise to such suspicion."); *United States v. Hampe*, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007) ("the peculiar facts presented in this case gave rise to a reasonable suspicion that Hampe's computer might contain child pornography"). The only case in which the court did not make an independent finding of reasonable suspicion was *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008).

[37] *Oversight of the Department of Homeland Security: Hearings Before the Senate Comm. On the Judiciary*, 110th Cong. 41-42 (2008) (testimony of Secretary of the Dep't of Homeland Security, Michael Chertoff) ("as a practical matter, when we look at a laptop or papers or something, it's because somebody is in secondary, which means by definition that we have a reasonable suspicion").

[38] See Travelers' Privacy Protection Act of 2008, S. 3612, 110th Cong. (2008) and Securing Our Borders and Our Data Act of 2009, H.R. 239, 11th Cong. (2009).

wireless phones, ipads and other tablet devices, ipods and MP3 players, blackberries and other wireless data devices, digital cameras, and any form of electronic, digital or other portable device used to store data.

2. Amend the Directives to clearly prohibit racial or religious profiling. The Directives should require that in determining whether reasonable suspicion exists, officials' analysis should focus on behaviors and any intelligence information or evidence of wrongdoing. Race, ethnicity, and religious affiliation should not be considered as factors that create suspicion unless these factors are used as part of a specific suspect description.

3. Amend the Directives to require that in the case of U.S. persons, CBP and ICE officials must obtain a warrant based on probable cause to (1) continue the search of an electronic device beyond a time period needed for a reasonable examination of the data, which is presumptively up to 24 hours, but should be based on what is actually reasonable under the circumstances; or (2) retain copies of the information or data contained on an electronic device for longer than 24 hours. If, however, officials believe the data may have intelligence value related to international terrorism and wish to seek a FISA search warrant, more time may be needed to complete that process. Thus, if officials have begun the process of seeking a FISA warrant during the 24 hour period described above, they should be permitted to retain the device for up to seven days if such additional time is needed to complete the process of seeking a FISA warrant.

4. Revise the ICE and CBP Directives to eliminate any differences between the type, standards for, and extent of searches permitted by the two policies.

5. Create and publish guidelines on handling and review of legally privileged information by CBP and ICE. "Legally privileged information" should include any information protected by the attorney-client privilege, attorney-work product doctrine, medical records or information, journalist's notes and information, and any other information protected by a recognized legal privilege.

6. Revise the Directives to provide that in the case of U.S. persons, the scope and nature of searches of electronic devices at the border, even when supported by reasonable suspicion, should be reasonably related to the underlying predicate for the search.

7. Conduct regular audits of the operation of these programs and regularly report to Congress on the findings. Such reports should include statistics on the number of people whose devices are searched, the number of devices detained beyond 24 hours, and the number of devices from which data was retained.

MEMBERS OF THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY COMMITTEE*

Endorsing *Suspicionless Border Searches of Electronic Devices*

CO-CHAIRS:

David Cole, Professor of Law, Georgetown University Law Center

David Keene, Former Chairman, American Conservative Union

MEMBERS:

Stephen E. Abraham, Lieutenant Colonel, Military Intelligence, United States Army Reserve (Ret.); Attorney, private practice

Azizah Y. al-Hibri, Professor, The T.C. Williams School of Law, University of Richmond; Founder and Chair of the Board, Karamah: Muslim Women Lawyers for Human Rights

Bob Barr, Former Member of Congress (R-GA); Practicing Attorney in Atlanta, GA; CEO, Liberty Strategies, Inc.

Phillip J. Cooper, Professor, Mark O. Hatfield School of Government, Portland State University

Mickey Edwards, Vice President, Aspen Institute; former member of Congress (R-OK) and chairman of the House Republican Policy Committee

Eugene R. Fidell, Florence Rogatz Lecturer in Law, Yale Law School

Michael German, Former Special Agent, Federal Bureau of Investigation

Philip Giraldi, Contributing Editor for *The American Conservative Magazine*, antiwar.com, and *Campaign for Liberty*; Executive Director, Council for the National Interest; former operations officer specializing in counter-terrorism, Central Intelligence Agency, 1975-1992; United States Army Intelligence

Asa Hutchinson, Senior Partner, Asa Hutchinson Law Group; Under Secretary for Border and Transportation Security, Department of Homeland Security, 2003-2005; Administrator, Drug Enforcement Administration, 2001-2003; Member of Congress, (R-AR), 1997-2001; United States Attorney, Western District of Arkansas, 1982-1985

David Lawrence, Jr., President, Early Childhood Initiative Foundation; Publisher (Ret.), *Miami Herald* and *Detroit Free Press*

Mary O. McCarthy, Consultant, Freedom of Information and Privacy Act; Associate Deputy Inspector General, Investigations, Central Intelligence Agency, 2005-2006; Visiting Fellow, Center for Strategic and International Studies, 2002 to 2004; Senior Policy Planner, Directorate

of Science and Technology, Central Intelligence Agency, 2001-2002; Senior Director, Special Assistant to the President, National Security Council, 1998-2001; Director for Intelligence Programs, National Security Council, 1996-1998; National Intelligence Officer for Warning, (Deputy 1991-1994) 1991-1996.

James E. McPherson, Rear Admiral, US Navy (Ret.); Judge Advocate General of the Navy, 2004-2006; Deputy Judge Advocate General of the Navy, 2002-2004; Active Duty, United States Navy, Judge Advocate General's Corps, 1981-2006

Paul R. Pillar, Visiting Professor and Director of Studies, Security Studies Program, Georgetown University; Intelligence officer (positions included Deputy Chief of DCI Counterterrorist Center, National Intelligence Officer for the Near East and South Asia, and Executive Assistant to the Director of Central Intelligence), Central Intelligence Agency and National Intelligence Council, 1977-2005

Peter Raven-Hansen, Glen Earl Weston Research Professor, George Washington University Law School

William S. Sessions, Partner, Holland and Knight LLP; Director, Federal Bureau of Investigation, 1987-1993; Judge, United States District Court for the Western District of Texas, 1974-1987, Chief Judge, 1980-1987; United States Attorney, Western District of Texas, 1971-1974

John W. Whitehead, President, The Rutherford Institute

Lawrence B. Wilkerson, Colonel, US Army (Ret.); Adjunct Professor of Government and Public Policy at the College of William and Mary; Chief of Staff to Secretary of State Colin L. Powell, 2002-2005

REPORTER:

Jay S. Brown, Mayer Brown LLP

THE CONSTITUTION PROJECT STAFF:

Sharon Bradford Franklin, Senior Counsel, Rule of Law Program

---

* *Affiliations listed for identification purposes only*

In the name of God, the Compassionate, the Merciful

Council on American-Islamic Relations
Washington State Chapter
9594 First Avenue Northeast, Suite 272, Seattle, Washington 98115
Telephone: 206.367.4081 www.cair.com

January 4, 2011

Secretary Janet Napolitano
U.S. Department of Homeland Security
Washington, DC 20528

RECEIVED BY CRS EXECUTIVE
2011 JAN -4 PM 12:59

Via U.S. Mail and Facsimile: 202.612.1976

Re: [redacted] border discrimination complaint

Dear Secretary Napolitano:

I hope this letter reaches you in the best of health and spirits. It is my unfortunate duty to report a case of discrimination by officers of Customs and Border Protection (CBP) against a member of the American Muslim community, [redacted]

[redacted] informed our office that on December 20th, 2010, he was handcuffed, unreasonably detained, had his person and car searched, and was questioned by CBP officers. [redacted] has authorized our office to address you on his behalf, and you will find his signed confidentiality waiver attached.

According to [redacted] he was returning from a brief vacation in Canada with his children, when he was stopped on December 20th, 2010, at the Peace Arch Border. [redacted] was stopped at the border around 1200 hours and asked to surrender his passport. [redacted] complied and reported that a CBP officer disappeared, with his passport, into a small office. When the officer returned, he instructed Mr. [redacted] to turn off his vehicle. The officer walked behind [redacted] vehicle and instructed [redacted] to reveal his hands, and then exit his vehicle with his hands up. After [redacted] emerged from his vehicle, he was handcuffed and relocated to a small, concrete room. [redacted] was extensively searched. CBP officers searched his person, clothes, wallet, shoes, cell phone, and vehicle.

When [redacted] inquired into the reason for his being stopped, CBP officers reportedly told Mr. [redacted] that a protection order had been issued against him, forbidding him from contacting his children. CBP officers also told [redacted] that the Seattle Police Department had notified them of this protection order.

[redacted] was detained for 15 minutes, during which CBP officers questioned [redacted] about his international travel. After being questioned, [redacted] was permitted to enter the United States with his children. When [redacted] returned to Seattle, he contacted the Seattle Police Department about the protection order issued against him. According the [redacted] the Seattle Police Department indicated that there was no protection order on [redacted] record.

[redacted] reported feeling humiliated by CBP officers when handcuffed in front of his children. Further, [redacted] did not receive an apology from CBP officers for wrongfully handcuffing and detaining him.

In the name of God, the Compassionate, the Merciful

Council on American-Islamic Relations
Washington's American Voice
9594 First Avenue Northeast, Suite 272, Seattle, Washington 98115
info@cair-research.org 206.367.4081 www.cair.com

42 U.S.C. § 1983 prohibits officers from using their authority to deprive individuals of federally protected rights as mandated by the Equal Protection Clause of the 14th Amendment of the United States Constitution. CAIR-WA has reviewed the facts of this case and has determined that Customs and Border Protection may have violated [redacted] civil rights including protection from unlawful searches and seizures under the 4th Amendment and equal protection guarantees of the 14th Amendment to the U.S. Constitution.

In light of recent Government actions of stereotyping and profiling of Muslims, it appears that Mr. [redacted] was unreasonably detained and searched simply on the basis of his perceived religion, race and/or ethnicity.

Therefore, CAIR-WA is requesting the following within 30 days of receipt of this letter:

1. Initiate an investigation into the incidents.
2. Provide [redacted] with a formal written apology for the treatment he received.
3. Provide [redacted] with monetary compensation for the mental, and emotional pain he and his children have suffered as a result of this incident.
4. Provide an explanation as to why [redacted] was handcuffed and detained on December 20th, 2010.
5. Institute CAIR's Workplace Sensitivity and Diversity Training for Customs and Border Protection officers.

The Council on American-Islamic Relations is a national civil rights organization whose mission is to defend the religious rights of Muslims in America. CAIR-Washington will continue to monitor this situation very closely and take any appropriate action that it deems necessary. We look forward to a swift and positive resolution.

In the meantime, please do not hesitate to reach me via e-mail at civilrights@wa.cair.com or via phone at 206.367.4081

Sincerely,

Jennifer Gist
Civil Rights Coordinator

In the name of God, the Compassionate, the Merciful

Council on American-Islamic Relations
Washington State Chapter
9594 First Avenue Northeast, Suite 272, Seattle, Washington 98115
info@cairseattle.org 206.367.4081 www.cair.com

Cc: Honorable Maria Cantwell, United States Senate
Honorable Patty Murray, United States Senate
Honorable Rick Larsen, House of Representatives, 2nd Congressional District
Honorable Jim McDermott, House of Representatives, 7th Congressional District
Honorable Chris Gregoire, Governor
Chief Marco Lopez, Chief of Staff, Customs and Border Protection
Mr. Alan Bersin, Commissioner, Customs and Border Protection
Mr. David V. Aguilar, Deputy Commissioner, Customs and Border Protection
Ms. Michele James, CBP Director of Field Operations
Mr. Greg Alvarez, Area Port Director
Mr. Mike Milne, Press Officer, Service Port at Blaine, Washington
Ms. Margo Schlanger, Officer for Civil Rights and Civil Liberties, Department of Homeland Security
Mr. Kareem Shora, Senior Policy Advisor, Department of Homeland Security
Mr. Brett Laduzinsky, Office of the Commissioner, Customs and Border Protection
Mr. Arsalan Bukhari, Executive Director, CAIR-Washington
(b)(6), (b)(7)(C) [redacted]

In the name of God, the Compassionate, the Merciful

Council on American-Islamic Relations
Washington State Chapter
9594 First Avenue Northeast, Suite 272, Seattle, Washington 98115
info@cairseattle.org 206.367.4081 www.cair.com

INFORMATION RELEASE STATEMENT

I, [redacted] residing at [redacted] authorize the Council on American-Islamic Relations ("CAIR") to be my agent and representative in regards to my complaint of discrimination and any related matter to the incident that occurred with/at The Border of US Side at Blain, WA

I hereby give CAIR and its representatives full authority to review, discuss, delegate and communicate all relevant and/or incidental information relating to my complaint.

I fully understand that I do not forfeit any of my legal rights and privileges as a condition to this agreement. I also understand that CAIR is not a legal services organization and I will neither hold CAIR financially or legally liable in respect to any subsequent judicial or administrative proceeding which may result from CAIR's involvement with my complaint.

I, the undersigned, hereby permit CAIR to investigate my complaint pursuant to the terms of the aforementioned agreement.

Sincerely,

[redacted]

(Signature)

01-03-2011

Date

CAIR

Council on American-Islamic Relations
Washington State Chapter
9594 First Avenue Northeast, # 272
Seattle, Washington 98115
info@cairseattle.org | 206.367.4081 | www.cair.com

FACSIMILE TRANSMITTAL SHEET

TO: SECRETARY JANET NAPOLITANO

FROM: COUNCIL ON AMERICAN-ISLAMIC RELATIONS OF WASHINGTON STATE (CAIR-WA)

COMPANY: DHS

DATE: 01.04.11

FAX NUMBER: 202.612.1976

TOTAL NO. OF PAGES: 5, INCLUDING COVER LETTER

PHONE NUMBER: 202.282.8000

PHONE NUMBER: 206.367.4081

RE: (b) (6), (b) (7)(C) [redacted] BORDER DISCRIMINATION COMPLAINT

☑ URGENT ☑ FOR REVIEW

☐ PLEASE COMMENT ☑ PLEASE REPLY

NOTES/COMMENTS:

The New York Times • Reprints

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers here or use the "Reprints" tool that appears next to any article. Visit www.nytreprints.com for samples and additional information. Order a reprint of this article now.

February 19, 2011

Can You Frisk a Hard Drive?

By DAVID K. SHIPLER

If you stand with the Customs and Border Protection officers who staff the passport booths at Dulles airport near the nation's capital, their task seems daunting. As a huge crowd of weary travelers shuffle along in serpentine lines, inspectors make quick decisions by asking a few questions (often across language barriers) and watching computer displays that don't go much beyond name, date of birth and codes for a previous customs problem or an outstanding arrest warrant.

The officers are supposed to pick out the possible smugglers, terrorists or child pornographers and send them to secondary screening.

The chosen few — 6.1 million of the 293 million who entered the United States in the year ending Sept. 30, 2010 — get a big letter written on their declaration forms: A for an agriculture check on foodstuffs, B for an immigration issue, and C for a luggage inspection. Into the computer the passport officers type the reasons for the selection, a heads-up to their colleagues in the back room, where more thorough databases are accessible.

And there is where concerns have developed about invasions of privacy, for the most complete records on the travelers may be the ones they are carrying: their laptop computers full of professional and personal e-mail messages, photographs, diaries, legal documents, tax returns, browsing histories and other windows into their lives far beyond anything that could be, or would be, stuffed into a suitcase for a trip abroad. Those revealing digital portraits can be immensely useful to inspectors, who now hunt for criminal activity and security threats by searching and copying people's hard drives, cellphones and other electronic devices, which are sometimes held for weeks of analysis.

Digital inspections raise constitutional questions about how robust the Fourth Amendment's guarantee "against unreasonable searches and seizures" should be on the border, especially in a time of terrorism. A total of 6,671 travelers, 2,995 of them American citizens, had electronic gear searched from Oct. 1, 2008, through June 2, 2010, just a tiny percentage of arrivals.

"But the government's obligation is to obey the Constitution all the time," said Catherine Crump, a lawyer for the American Civil Liberties Union. "Moreover, controversial government programs often start small and then grow," after which "the government argues that it is merely carrying out the same policies it has been carrying out for years."

One of the regular targets is Pascal Abidor, a Brooklyn-born student getting his Ph.D. in Islamic studies, who reported being frisked, handcuffed, taken off a train from Montreal and locked for several hours in a cell last May, apparently because his computer contained research material in Arabic and news photographs of Hezbollah and Hamas rallies. He said he was questioned about his political and religious views, and his laptop was held for 11 days.

Another is James Yee, a former Muslim chaplain at the Guantánamo Bay prison, who gets what he wryly calls a "V.I.P. escort" whenever he flies into the United States. In 2003, Mr. Yee was jailed and then exonerated by the Army after he had conveyed prisoners' complaints about abuse, urged respect for their religious practices and reported obscene anti-Muslim caricatures being e-mailed among security staff.

Years later, he evidently remains on a "lookout" list. A federal agent stands at the door of Mr. Yee's incoming plane, then escorts him to the front of the passport line and to secondary screening.

Arriving in Los Angeles last May from speaking engagements in Malaysia, he was thoroughly questioned and searched, he said, and his laptop was taken for three or four hours. He was not told why, but after it was returned and he was waiting to rebook a connecting flight he'd missed, a customs officer rushed up to the counter. "We left our disk inside your computer," he quoted her as saying. "I said, 'It's mine now.' She said no, and sure enough when I took the computer out, there was a disk."

Customs won't comment on specific cases. "The privacy rights that citizens have really supersede the government's ability to go into any depth," said Kelly Ivahnenko, a

spokeswoman.

In general, "we're looking for anyone who might be violating a U.S. law and is posing a threat to the country," she explained. "We're in the business of risk mitigation."

Yet the mitigation itself has created a sense of risk among certain travelers, including lawyers who need to protect attorney-client privilege, business people with proprietary information, researchers who promise their subjects anonymity and photojournalists who may pledge to blur a face to conceal an identity. Some are now taking precautions to minimize data on computers they take overseas.

"I just had to do this myself when I traveled internationally," said Ms. Crump, the lead attorney in a lawsuit challenging the policy on behalf of Mr. Abidor, the National Association of Criminal Defense Lawyers and the National Press Photographers Association.

During a week in Paris, where she lectured on communications privacy, she had legal work to do for clients, which she could not risk the government seeing as she returned. "It's a pain to get a new computer," she said, "wipe it completely clean, travel through the border, put the new data on, wipe it completely clean again."

In simpler days, as customs merely looked for drugs, ivory, undeclared diamonds and other contraband that could be held in an inspector's hand, searches had clear boundaries and unambiguous results.

Either the traveler had banned items, or didn't. Digital information is different. Some is clearly illegal, some only hints at criminal intent, and under existing law, all is vulnerable to the same inspection as hand-carried material on paper.

Most pirated intellectual property and child pornography, for example, cannot be uncovered without fishing around in hard drives. "We've seen a raft of people coming from Southeast Asia with kiddie porn," said Christopher Downing, a supervisor at Dulles. If a person has been gone only two or three days and pictures of children are spotted in a bag, he explained, the laptop is a logical candidate for inspection. Such searches have been fruitful, judging by the bureau's spreadsheets, which list numerous child pornography cases.

But terrorism is an amalgam of violence and ideas, so its potential is harder to define as officers

scrutinize words and images as indicators of attitudes, affiliations and aspirations. Random searches are not done, Mr. Downing said, although courts so far have upheld computer inspections without any suspicion of wrongdoing. In practice, something needs to spark an officer's interest. "If you open up a suitcase and see a picture of somebody holding an RPG," he noted, referring to a rocket-propelled grenade, "you'd want to look into that a little more."

The search power is preserved by its judicious use, Mr. Downing said. "If you abuse it, you lose it." he added. The A.C.L.U. doesn't want customs to lose it, Ms. Crump explained, but just wants the courts to require reasonable suspicion, as the Supreme Court did in 1985 for examinations of a person's "alimentary canal." The court distinguished such intrusive inspection from "routine searches" on the border, which "are not subject to any requirement of reasonable suspicion, probable cause, or warrant." The justices added in a footnote that they were not deciding "what level of suspicion, if any, is required for nonroutine border searches" of other kinds.

Laptop searches should be considered "nonroutine," Ms. Crump argues, something the United States Court of Appeals for the Ninth Circuit declined to do in 2008, when it reversed a judge's decision to suppress evidence of child pornography obtained during a suspicionless airport computer search.

With the search powers intact, Mr. Abidor no longer dares take the train home from his studies at McGill University in Montreal. He doesn't want to be stranded at the border, waiting hours for a bus, as he was in May. So last month his father drove up from New York to get him for vacation. The men were ordered to a room and told to keep their hands on a table while customs officers spent 45 minutes searching the car, and possibly the laptop, Mr. Abidor said. "I was told to expect this every time."

David K. Shipler, a former reporter at The Times, is the author of "The Rights of the People: How Our Search for Safety Invades Our Liberties," to be published in April.