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*