Border Searches of Laptop Computers and Other Electronic Storage Devices

Yule Kim
Legislative Attorney

November 16, 2009

Congressional Research Service
7-5700
www.crs.gov
RL34404

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

As a general rule, the Fourth Amendment of the U.S. Constitution requires government-conducted searches and seizures to be supported by probable cause and a warrant. Federal courts have long recognized that there are many exceptions to these requirements, one of which is the border search exception. The border search exception permits government officials to conduct "routine" searches based on no suspicion of wrongdoing whatsoever. On the other hand, when warrantless border searches are particularly invasive, and thus "non-routine," they are permissible only when customs officials have, at a minimum, a "reasonable suspicion" of wrongdoing.

The federal courts that have addressed this issue have held that the border search exception applies to searches of laptops at the border. Although the Supreme Court has not directly addressed the degree of suspicion needed to search laptops at the border without a warrant, the federal appellate courts that have addressed the issue appear to have concluded that reasonable suspicion is not needed to justify such a search. The Ninth Circuit, in *United States v. Arnold*, explicitly held that reasonable suspicion is not required to conduct a warrantless search of a laptop at the border.

Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE), two agencies within the Department of Homeland Security (DHS) that have roles in border security, have published directives outlining their policies and procedures regarding laptop border searches. Both policies assert that, as a general matter, laptop border searches may be conducted without any individualized suspicion and require reasonable suspicion only in certain circumstances.

A bill introduced in the 111th Congress, the Securing our Borders and our Data Act of 2009 (H.R. 239), would impose more rigorous standards for laptop searches than those the federal courts have determined are constitutionally required. Another bill introduced in the 111th Congress, the Border Security Search Accountability Act of 2009 (H.R. 1726), would mandate that the Commissioner of Customs and Border Protection promulgate a rule with respect to the scope of and procedural and record keeping requirements associated with border security searches of electronic devices.

Contents

Contacts

Introduction

A developing issue in the law of search and seizure is whether the Fourth Amendment of the U.S. Constitution permits warrantless searches of the content of laptop computers and other electronic storage devices at U.S. borders. The federal courts that have addressed this issue have held that the border search exception to the Fourth Amendment applies to these searches, making warrantless searches permissible. Although most of these courts did not make explicit the degree of suspicion needed to initiate such a search, the United States Court of Appeals for the Ninth Circuit ruled that the Fourth Amendment does not require reasonable suspicion, or, for that matter, any suspicion of wrongdoing at all, to justify a warrantless search of laptops at the border.

Border Search Exception

The Fourth Amendment mandates that a search or seizure conducted by a government agent must be "reasonable."[1] As a general rule, courts have construed Fourth Amendment *reasonableness* as requiring probable cause[2] and a judicially granted warrant.[3] Nonetheless, the Supreme Court has recognized several exceptions to these requirements, one of which is the border search exception.[4]

The border search exception to the Fourth Amendment allows federal government officials to conduct searches at the border without a warrant or probable cause. Although Congress and the federal courts have long assumed, at least implicitly, the existence of a border search exception,[5] the Supreme Court did not formally recognize it until it decided *Ramsey v. United States* in 1977.[6] In *Ramsey*, the Supreme Court approved the search of several suspicious envelopes (later found to contain heroin) conducted by a customs official pursuant to search powers authorized by statute.[7] The Court determined that the customs official had "reasonable cause to suspect"[8]

---

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

[2] The Supreme Court has interpreted *probable cause* to mean "a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). *See also* Ornelas v. United States, 517 U.S. 690, 696 (1996).

[3] Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process without prior approval by judge or magistrate are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well delineated exceptions.").

[4] For a more expansive treatment of the border search exception to the Fourth Amendment, see CRS Report RL31826, *Protecting the U.S. Perimeter: Border Searches Under the Fourth Amendment*, by Yule Kim.

[5] *See* Act of July 31, 1789, ch. 5 §§23-24, 1 Stat. 29, 43 (authorizing customs officials "full power and authority" to enter and search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed ..."); Carroll v. United States, 267 U.S. 132, 153-154 (1925) ("Travellers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in."). *Accord* Almeida-Sanchez v. United States, 413 U.S. 266 (1973); United States v. 12 200-Ft. Reels of Super 8mm. Film, 413 U.S. 123 (1973); United States v. Thirty-Seven (37) Photographs, 402 U.S. 363 (1971); Boyd v. United States, 116 U.S. 616 (1886).

[6] 431 U.S. 606, 619 (1977).

[7] *Id.* at 622.

[8] "Reasonable cause to suspect" appears to be equivalent to "reasonable suspicion," which is simply a particularized and objective basis for suspecting the particular person of wrongdoing. *See* Terry v. Ohio, 392 U.S. 1, 21 (1978).

suspicious activity when searching the envelopes.[9] This standard, while less stringent than probable cause, was sufficient justification.[10] The border search exception has subsequently been expanded beyond persons, objects, and mail entering the United States, to cover individuals and objects departing from the United States[11] and to apply in places deemed the "functional equivalent" of a border, such as international airports.[12]

As the border search exception has further developed in case law, lower federal courts have recognized two different categories of border searches: routine and non-routine. This distinction is based on language in *United States v. Montoya de Hernandez*, where the Supreme Court determined the level of suspicion needed to justify "a seizure of an incoming traveler for purposes other than a routine border search."[13] In that case, customs officials detained a traveler whom they suspected of smuggling drugs.[14] The customs officials eventually obtained a court order authorizing a rectal examination, which produced a balloon containing cocaine.[15] The Court held that, even though the detention "was beyond the scope of a routine customs search and inspection," the customs officials' "reasonable suspicion" that the suspect was smuggling drugs provided sufficient justification for the search.[16] Federal courts have since interpreted this case to stand for the proposition that "reasonable suspicion" (i.e., a particularized and objective basis for suspecting wrongdoing) is required to justify similarly invasive searches.[17]

Although the Court in *Montoya de Hernandez* focused on a "non-routine" detention of a traveler at the border, lower federal courts, interpreting *dictum* in that case, began distinguishing unusually intrusive searches from "routine" searches.[18] These courts thereby expanded the border search exception by concluding that a customs official may conduct "routine" warrantless searches of persons or effects without any reason for suspicion.[19] The Supreme Court further

[9] 431 U.S. at 614.

[10] *Id.* at 619 ("This 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.").

[11] *See* United States v. Berisha, 925 F.2d 791, 795 (5th Cir. 1991) (extending the border search exception to routine outbound searches); United States v. Stanley, 545 F.2d 661, 667 (9th Cir. 1976), *cert. denied*, 436 U.S. 917 (1978); United States v. Ezeiruaku, 936 F.2d 136, 143 (3d Cir. 1991); United States v. Duncan, 693 F.2d 971, 977 (9th Cir. 1982); United States v. Ajlouny, 629 F.2d 830, 834 (2d Cir. 1980).

[12] *See* Almeida-Sanchez v. United States, 413 U.S. 266, 272-273 (1973); United States v. Hill, 939 F.2d 934, 936 (11th Cir. 1991); United States v. Gaviria, 805 F.2d 1108, 1112 (2d Cir. 1986). In the context of international airports, the border search exception only applies to searches of persons and effects on international flights, whereas the administrative search exception, which applies to routine searches with purposes unrelated to law enforcement, is used to justify searches of persons and effects on domestic flights. *See* United States v. Davis, 482 F.2d 893, 908-912 (9th Cir. 1973).

[13] 473 U.S. 531, 541 (1985) ("We have not previously decided what level of suspicion would justify a seizure of an incoming traveler for purposes other than a routine border search.").

[14] *Id.* at 535.

[15] *Id.*

[16] *Id.* at 541 ("We hold that the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal.").

[17] *See* United States v. Flores-Montano, 541 U.S. 149, 154 *citing Terry*, 392 U.S. at 21 ("And in justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.").

[18] *Montoya de Hernandez*, 473 U.S. at 538 ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant, and first-class mail may be opened without a warrant on less than probable cause.").

[19] *See* United States v. Ezeiruaku, 936 F.2d 136 (3d Cir. 1991); *Berisha*, 925 F.2d 791. *See also* United States v. (continued...)

developed this doctrine in *United States v. Flores-Montano*, in which it held that the disassembly and examination of an automobile gasoline tank at the border did not have to be justified by any suspicion of wrongdoing.[20] The Court concluded that the gasoline tank search was no more intrusive than a routine vehicle search because there was no heightened expectation of privacy surrounding the contents of a gasoline tank; this conclusion was reached even though the search involved a time-consuming disassembly of the vehicle.[21] *Flores-Montano* illustrates that extensive, time-consuming, and potentially destructive warrantless searches of objects and effects can be conducted without any reasonable suspicion of wrongdoing.

In summary, Supreme Court precedent currently indicates that federal border officers do not need any suspicion of wrongdoing to support most border searches. An exception arises, however, with respect to highly intrusive, non-routine searches. These searches require "reasonable suspicion."[22] Yet, the precise level of intrusion that would render a border search non-routine is undefined in the case law.[23] Typically, this question is dealt with in a fact-specific manner on a case-by-case basis.[24] Nonetheless, *Flores-Montano* indicates that, unlike a search of a person's body, intrusiveness may not be a dispositive factor when determining whether the search of a vehicle or personal effects requires reasonable suspicion. Thus, it appears that in most cases, courts are likely to uphold that even very invasive searches of personal property can be conducted without a warrant and be based on no suspicion whatsoever.[25]

Judicial Developments on Laptop Searches

With the advent of portable computing, it is now common practice for travelers to store their data on laptop computers, compact discs, and other electronic storage devices and to travel with them across the U.S. border. In response, customs officials have been searching and seizing such devices. The issue confronting federal courts is whether the border search exception applies to electronic storage devices, and if it does, what degree of suspicion is needed to justify a warrantless search.

The Supreme Court has yet to address this issue. Most lower federal courts, however, have concluded that searches of laptops, computer disks, and other electronic storage devices fall under

---

(...continued)

Chaplinksi, 579 F.2d 373 (5th Cir. 1978); United States v. Lincoln, 494 F.2d 833 (9th Cir. 1974); United States v. Chavarria, 493 F.2d 935 (5th Cir. 1974); United States v. King, 483 F.2d 353 (10th Cir. 1973).

[20] 541 U.S. 149, 154 (2004).

[21] *Id.* ("It is difficult to imagine how the search of a gas tank, which should be solely a repository for fuel, could be more of an invasion of privacy than the search of the automobile's passenger compartment.").

[22] *See id. citing Terry*, 392 U.S. at 21 ("And in justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.").

[23] *See id.* at 541 n. 4.

[24] *Id.* (requiring "reasonable suspicion" for the detention of a traveler at the border, beyond the scope of a routine customs search and inspection). *See also* Henderson v. United States, 390 F.2d 805 (9th Cir. 1967) (holding that strip searches may be conducted only upon a real suspicion); United States v. Adekunle, 980 F.2d 985 (5th Cir. 1992), on reh'g, 2 F.3d 559 (5th Cir. 1993) (requiring reasonable suspicion to justify a strip search); United States v. Asbury, 586 F.2d 973, 975-976 (2d Cir. 1978) (requiring reasonable suspicion for strip searches); Rivas v. United States, 368 F.2d 703 (9th Cir. 1966) (requiring a clear indication of the possession of narcotics to justify an alimentary canal search).

[25] *Flores-Montano*, 541 U.S. at 152.

the border search exception, which means neither a warrant nor probable cause is necessary to support the search.[26] Nonetheless, these courts have not explicitly established the degree of suspicion required to justify a warrantless search of a laptop at the border; rather, courts have avoided the issue by finding that reasonable suspicion supported the particular searches before them.[27] Even in the one instance a court held that a laptop search was routine, it also found that reasonable suspicion supported the search.[28] The one exception to this trend is *United States v. Arnold*, in which the Ninth Circuit explicitly held that reasonable suspicion was not needed to support a warrantless border search of laptops and other electronic storage devices.[29] Because laptop border search cases are a developing area of case law, a full understanding of this issue requires a closer look at the facts of these cases and the approaches the courts used in their analyses.

United States v. Ickes

One of the first federal appellate cases to discuss searches of laptops at the border is *United States v. Ickes*.[30] In *Ickes*, a customs official, without a warrant, searched the defendant's van near the Canadian border after discovering during a routine search a videotape that focused excessively on a young ballboy during a tennis match.[31] His suspicions raised, the official requested the assistance of a colleague. They then proceeded to conduct a more thorough search in which they uncovered marijuana paraphernalia, a photo album containing child pornography, a computer, and several computer disks.[32] Other customs officials proceeded to examine the contents of the computer and disks, all of which contained additional child pornography.[33] The defendant later filed a motion, which was denied by the trial court, seeking to suppress the contents of the computer and disks on both First and Fourth Amendment grounds.[34]

The Fourth Circuit held that the search of the defendant's computer and disks did not violate either the Fourth or First Amendment. Regarding the Fourth Amendment challenge, the court noted that the border search exception applied in this case.[35] The court concluded by opining that

---

[26] *See, e.g.*, United States v. Ickes, 393 F.3d 501, 505 (4th Cir. 2005); United States v. Romm, 455 F.3d 990, 997 (9th Cir. 2006); United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006) ("An airport is considered the functional equivalent of a border and thus a search there may fit within the border search exception."); United States v. Furukawa, No. 06-145, slip op. (D. Minn., November 16, 2006), 2006 U.S. Dist. LEXIS 83767; United States v. Hampe, No. 07-3-B-W, slip op. (D. Me., April 18, 2007), 2007 U.S. Dist. LEXIS 29218.

[27] *See, e.g.*, *Irving*, 452 F.3d at 124 ("Because these searches were supported by reasonable suspicion, we need not determine whether they were routine or non-routine."); *Furukawa*, slip op. at *1-2 ("[T]he court need not determine whether a border search of a laptop is 'routine' for purposes of the Fourth Amendment because, regardless, the magistrate judge correctly found the customs official had a reasonable suspicion in this case.").

[28] *Ickes*, 393 F.3d at 507 (noting that the computer search did not begin until the customs agents found marijuana paraphernalia and child pornography which raised a reasonable suspicion); *Hampe*, slip op. at *4-5 (holding that even though the laptop search did not implicate any of the serious concerns that would characterize a search as non-routine, the peculiar facts of the case gave rise to reasonable suspicion).

[29] 533 F.3d 1003, 1008 (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.").

[30] 393 F.3d 501 (4th Cir. 2005).

[31] *Id.* at 502.

[32] *Id.* at 503.

[33] *Id.*

[34] *Id.*

[35] *Id.* at 505.

"[a]s a practical matter, computer searches are most likely to occur where—as here—the traveler's conduct or the presence of other items in his possession suggest the need to search further," indicating that the court believed that such searches will typically occur only when a customs official has reasonable suspicion.[36]

The court also rejected the defendant's contention that the First Amendment bars the border search exception from being applied to "expressive" materials. The court stated that a First Amendment exception would "create a sanctuary for all expressive materials—including terrorist plans," and that it would cause an excessive amount of administrative difficulties for those who would have to enforce it.[37]

United States v. Romm

The Ninth Circuit has also addressed this issue in *United States v. Romm*.[38] The defendant in that case had arrived at an airport in British Columbia when a Canadian customs agent, after discovering that he had a criminal history, searched the defendant's laptop.[39] During the search, the Canadian customs agent uncovered child pornography sites in the laptop's "internet history"; the defendant was consequently denied entry into Canada and flown to Seattle.[40] The Canadian authorities informed U.S. Immigration and Customs Enforcement (ICE) of the contents of the defendant's laptop. When the defendant arrived in Seattle, ICE detained the defendant and convinced him to allow ICE agents to examine his laptop without a warrant.[41] ICE agents then used a forensic analysis, which recovered deleted child pornography from the laptop. The defendant later filed a motion to suppress the evidence obtained from his laptop, which the trial court denied.[42]

The Ninth Circuit held that the forensic analysis used by the ICE agents fell under the border search exception.[43] The court noted that airport terminals were "the functional equivalents" of a border, allowing customs agents to conduct routine border searches of all deplaning passengers.[44] The court then stated that all passengers deplaning from an international flight are subject to "routine" border searches.[45] Because the defendant failed to brief the argument that the First Amendment implications of warrantless laptop searches render such searches "non-routine," the court did not consider that argument.[46] The court instead presumed that the search of the defendant's laptop was a part of a "routine" search conducted after deplaning from an international flight.[47] However, because the court made this conclusion solely because the

[36] *Id.* at 507.

[37] *Id.* at 506.

[38] 455 F.3d 990 (9th Cir. 2006).

[39] *Id.* at 994.

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.* at 997.

[44] *Id.* at 996.

[45] *Id.*

[46] *Id.*

[47] *Id.* at 997.

defendant failed to brief his argument, the court's determination that the search was "routine" had no precedential effect.[48]

United States v. Arnold

In *United States v. Arnold*, another Ninth Circuit case, the court, apparently disregarding the traditional routine/non-routine distinction used in most border search cases, expressly held that reasonable suspicion was not required to support the warrantless laptop border search at issue.[49] Here, the defendant had returned from the Philippines when he underwent secondary questioning at the airport after having passed through the first customs checkpoint.[50] The customs agent, without a warrant, ordered the defendant to "turn on the computer so she could see if it was functioning."[51] While the defendant's luggage was being inspected, another customs agent searched the laptop's contents and found pictures of nude adult women.[52] The defendant was then detained for several hours while special agents from ICE conducted a more extensive search of the laptop and discovered material they believed to be child pornography.[53]

The Ninth Circuit first stated that warrantless "searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment."[54] Nonetheless, the court noted that the Supreme Court has recognized two situations where reasonable suspicion is required to conduct a search of personal property: (1) when the search is destructive, and (2) when the search is conducted in a particularly offensive manner.[55] Outside of these two situations, reasonable suspicion is not required to search property, regardless of the nature of the property being searched. Thus, the Ninth Circuit refused to take into consideration any special qualities of laptops that may distinguish them from other containers, such as a laptop's capability of storing large amounts of private data. Indeed, the court did not find the search of a laptop to be intrinsically "offensive" simply because a laptop had a large storage capacity.[56] Instead, the court treated border searches of laptops no differently from border searches of any other type of personal property.[57]

The Ninth Circuit, in its analysis, rejected the use of an "intrusiveness analysis." An intrusiveness analysis would require a customs officer to evaluate the potential intrusiveness of each search he wished to conduct on a case-by-case basis in order to determine whether reasonable suspicion would be needed to justify the search.[58] The court instead adopted a categorical approach to warrantless border searches: so long as the search is of a physical object rather than a person's body, reasonable suspicion is not required if the search is not physically destructive or particularly offensive.

---

[48] *Id.* (declining to consider the issue because arguments not raised by a party in its opening briefs are deemed waived).

[49] 533 F.3d 1003 (9th Cir. 2008).

[50] *Id.* at 1005.

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.* at 1007.

[55] *Id.* at 1007-1008.

[56] *Id.* at 1009.

[57] *Id.*

[58] *Id.* at 1008.

The Ninth Circuit also refused to apply a "least restrictive means" test to evaluate the constitutionality of a border agent's chosen method of conducting the search.[59] Thus, under the court's analysis, a border agent seemingly can conduct a search without having to determine whether a less intrusive means is available. The argument in favor of this categorical approach is that it appears easier for border agents to follow. On the other hand, the breadth of the Ninth Circuit's ruling apparently allows border agents, so long as they avoid searching a person's body, almost total discretion in determining both when, and in what manner, they may search personal property.

Finally, the Ninth Circuit refused to recognize a First Amendment protection of expressive materials searched at the border. Similar to the reasoning in *Ickes*, the court held that doing so could protect terrorist communications, create an unworkable standard for government agents, and contravene Supreme Court precedent.[60]

United States v. Seljan

The majority opinion in *United States v. Seljan* reaffirmed *Arnold* by holding that an incidental search of a letter's content at the border did not require reasonable suspicion.[61] However, a dissent by Judge Alex Kozinski argued that reasonable suspicion was required because a letter contains personal thoughts that the letter's author would expect to be normally immune from search, especially absent suspicion of wrongdoing. Although the facts of this case only involve letters, the analyses of both the majority and dissenting opinions address the search of text, and thus would seem to apply to written communications generally, including electronic communications.

In this case, a customs official discovered a letter soliciting sex from a child while searching a package being mailed to the Philippines. The search of the letter's contents was upheld even though the scope of the statute authorizing the search was limited to the interdiction of undeclared currency transported across the U.S. border.[62] Indeed, the *Seljan* majority specifically cited *Ramsey*, arguably the seminal case concerning the border search doctrine, in holding that "an envelope containing personal correspondence is not uniquely protected from search at the border."[63] Moreover, the court found additional justification for the search by concluding that it was not unreasonable under the circumstances because the customs official did not "read" the contents of the letter. Rather, he merely "scanned" it with his eyes, which then gave rise to the reasonable suspicion of unlawful conduct that justified a more exacting examination of the letter's contents.[64]

In contrast, Judge Kozinksi, in his dissent, argued that the Fourth Amendment provides heightened protections for expressive materials at the border.[65] He made two arguments to support this proposition. The first is based on the Fourth Amendment's text, which contains a specific prohibition against the unreasonable search and seizure of "papers." Judge Kozinski

[59] *Id.*

[60] *Id.* at 1010.

[61] 547 F.3d 993 (9th Cir. 2008).

[62] *Id.* at 996.

[63] *Id.* at 1003.

[64] *Id.* at 1004.

[65] *Id.* at 1014 (Kozinski, J., dissenting).

argued that this specific prohibition signals the Framers' desire to insulate expressive content, and the personal thoughts contained therein, from unnecessary government search.[66] In support of this interpretation, Judge Kozinski cited *Entick v. Carrington*, an English common law case which would have been familiar to the Framers, which rejected "the government's claim of unrestrained power to search personal papers" and held that the searches and seizures of documents violated English common law.[67] According to his analysis, the prevailing view at the time of *Entick* was that a search of private papers was every bit as intrusive as a body search, which, if accurate, would indicate that the Framers intended individualized suspicion to be required to support a search of papers even at the border.[68] Second, Judge Kozinski also distinguished *Seljan* from past Supreme Court precedent by characterizing the border search exception as a means to facilitate the interdiction of smuggled contraband.[69] Thus, according to Judge Kozinski, the border search exception should be limited to the search of "containers," primarily for the purpose of uncovering contraband, and should not be applied to facilitate the search of expressive materials.[70]

Federal Policies on Border Laptop Searches

Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) have issued directives outlining their policies and procedures regarding the border searches of laptops and other electronic devices. Both CBP and ICE are agencies within the Department of Homeland Security (DHS). CBP provides security at the U.S. borders and ports of entry by inspecting incoming persons and cargo in order to prevent the entry of certain individuals and goods, such as terrorists, unauthorized immigrants, contraband (i.e., illegal narcotics), and agricultural goods contaminated with pests or disease. ICE investigates individuals and criminal networks suspected of facilitating illegal activities such as unauthorized immigration, terrorism, and contraband smuggling.[71] Both directives assert that CBP and ICE do not require any individualized suspicion to search laptops and other electronic devices at the border, and outline similar procedures regarding the handling of seized materials.[72]

Customs and Border Protection Policy

U.S. Customs and Border Protection (CBP), the primary agency entrusted with border security, has released a "Directive" outlining the procedures "all CBP Officers, Border Patrol Agents, Interdiction Agents, Marine Interdiction Agents, and other employees authorized by law to perform searches at the border or the functional equivalent of the border, or the extended border"

[66] *Id.* at 1017-1019 (Kozinski, J., dissenting).

[67] *Id.* at 1017 (Kozinksi, J., dissenting) *citing Entick v. Harrington*, 19 Howell's State Trials 1029, 95 Eng. Rep. 807 (1765).

[68] *Id.* (Kozinski, J., dissenting).

[69] *Id.* at 1016. (Kozinski, J., dissenting).

[70] *Id.* at 1014-1015 (Kozinski, J., dissenting).

[71] For more details on CBP and ICE, *see generally* CRS Report RS21899, *Border Security: Key Agencies and Their Missions*, by Chad C. Haddal.

[72] Presumably, an *individualized suspicion* standard is synonymous with or perhaps even weaker than a *reasonable suspicion* standard. This is because the Supreme Court has rebuked the use by lower federal courts of standards of suspicion other than *probable cause* or *reasonable suspicion. See Montoya de Hernandez*, 473 U.S. at 541.

must follow when conducting border searches of laptops. This Directive, dated August 20, 2009, contains

> [g]uidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices, encountered by [CBP] at the border, both inbound and outbound, to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce.[73]

The Directive is limited to CBP's border search authority, and is not meant to limit CBP's authority to conduct other lawful searches at the border, such as those conducted pursuant to a warrant, consent, or incident to an arrest. It also is not intended to govern searches of commercial quantities of electronic devices (i.e., those transported in a shipping container).[74]

The Directive states that CBP officers may, with or without individualized suspicion, during the course of a border search examine an electronic device and analyze the information it contains. Furthermore, such searches should be conducted in the presence of the individual whose information is being examined unless "there are national security, law enforcement, or other operational considerations" to render the individual's presence during the search inappropriate. However, the Directive contains a caveat that an individual's presence does not necessarily mean the individual can witness the search itself, and an individual will not be allowed to witness the search if "law enforcement techniques or other operational considerations" stand to be compromised.[75]

The Directive also outlines procedures related to the search of privileged or other sensitive materials. Under the directive, legal materials, medical records, journalist work-related information, and business or commercial information may all be subject to search.[76] Legal materials are subject to special handling procedures. Specifically, if a CBP officer encounters legal materials he suspects may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP (e.g., customs searches or immigration inspection), the officer must first consult with the CBP Associate/Assistant Chief Counsel before searching the material.[77]

Medical records and journalist work-related information shall be handled in accordance with "any applicable federal law and CBP policy."[78] All business and commercial information encountered by CBP officers shall be treated as confidential and officers shall protect this information from unauthorized disclosures.[79] If a CBP officer has questions related to the review of these categories of information, they may be directed to the CBP Associate/Assistant Chief Counsel.[80]

---

[73] Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-049, § 1 (August 20, 2009).

[74] *Id.* at § 2 (August 20, 2009).

[75] Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-049, § 5.1 (August 20, 2009).

[76] *Id.* at § 5.2.

[77] *Id.* at § 5.2.1.

[78] *Id.* at § 5.2.2.

[79] *Id.* at § 5.2.3.

[80] *Id.* at §§ 5.2.2, 5.2.3.

Detention and review policies are also dictated by the Directive. It states that an officer "may detain electronic devices, or copies of information contained herein, for a brief, reasonable period of time to perform a thorough border search."[81] This search may take place on-site or off-site and should not exceed five days.[82] However, detentions may be extended by five days if approved by a Port Director, Patrol Agent in Charge, or other equivalent-level manager, and they can exceed 15 days if approved by "the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or other equivalent manager." Thereafter, extensions may be approved and re-approved in increments of seven days.[83] Furthermore, if review of the information reveals there is no probable cause to seize it, all copies of the information must be destroyed no later than seven days after the no probable cause determination is made, unless a supervisor approves an extension, which can last no longer than 21 days.[84]

The Directive also claims the right to use "other federal agency analytical resources outside of CBP and ICE, such as translation, decryption, and subject matter expertise."[85] Technical assistance (i.e., assistance in operating the electronic device for search or assistance in translating or decrypting the information), can be acquired from another federal agency without individualized suspicion. Assistance for "subject matter expertise" from experts working in other federal agencies may be had only when there is reasonable suspicion of activities in violation of the laws enforced by CBP. The Directive states that reasonable suspicion may be based upon the presence of an individual on a government terrorist watch list.[86]

If probable cause arises after the border search of information, CBP officers are authorized to seize the electronic device being searched, or to make copies of the information from the device. If probable cause does not arise, "CBP may retain only information relating 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."[87]

Immigration and Customs Enforcement Policy

Immigration and Customs Enforcement (ICE), the agency responsible for ensuring compliance with the federal immigration and customs laws, issued a directive on August 18, 2009, outlining the agency's policy and procedures regarding "the border search authority to search, detain, seize, retain, and share information contained in electronic devices possessed by individuals at the border, the functional equivalent of the border, and the extended border to ensure compliance with customs, immigration, and other laws enforced by ICE."[88]

[81] *Id.* at § 5.3.1.

[82] *Id.*

[83] *Id.* at § 5.3.1.1.

[84] *Id.* at § 5.3.1.2.

[85] *Id.* at §5.3.2.

[86] *Id.*

[87] *Id.* at § 5.4.

[88] Border Searches of Electronic Devices, ICE Directive No. 7-6.1, § 1.1 (August 18, 2009).

The Directive asserts that "ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion …"[89]

The Directive states that consent is not needed to conduct a border search.[90] However, ICE Special Agents should conduct border searches "in the presence of, or with the knowledge of, the traveler" to the extent practicable.[91] When not practicable, because of "law enforcement, national security, or other operational concerns," ICE Special Agents must note the circumstances in appropriate ICE systems.[92] In addition, permitting an individual to be in the room where the search is conducted does not mean the individual will be allowed to witness the search. If allowing the individual to witness the search could reveal "law enforcement techniques or potentially compromise other operational concerns," the individual will not be permitted to witness the search.[93]

The Directive states that "Special Agents are to complete the search of detained electronic devices, or copies of information therefrom, in a reasonable time given the facts and circumstances of the particular search" with the circumstances noted.[94] Searches are "generally" to be finished within 30 days of the date of detention, unless circumstances warrant extra time. Any detention exceeding the 30 calendar days must be approved by a Group Supervisor or equivalent, and approved every 15 calendar days thereafter, with the specific justification for additional time noted.[95]

The Directive outlines the procedures ICE Special Agents must use when seeking assistance from other federal agencies or non-federal entities. According to the procedure, Special Agents are "responsible for ensuring that the results of the assistance are received in a reasonable time."[96] Special assistance may be required when a Special Agent, during the course of a border search, encounters information in an electronic device that "presents technical difficulties, is in a foreign language, and/or is encrypted."[97] Special Agents may demand "translation, decryption, and/or technical assistance" from other federal agencies or non-federal entities.[98] This demand may be made without individualized suspicion.[99] Special Agents may also encounter information that requires subject matter experts to determine whether the information is relevant to the laws enforced by ICE.[100] This demand can be made when a Special Agent has reasonable suspicion that a law enforced by ICE is being violated.[101] Special Agents may create and transmit copies of information to other federal agencies or non-federal entities for subject matter assistance.

[89] *Id.* at § 6.1.
[90] *Id.* at § 8.1(3).
[91] *Id.* at § 8.1(2).
[92] *Id.*
[93] *Id.*
[94] *Id.* at § 8.3(1).
[95] *Id.*
[96] *Id.* at § 8.3(2).
[97] *Id.* at § 8.4(1)(a).
[98] *Id.*
[99] *Id.*
[100] *Id.* at § 8.4(2)(a).
[101] *Id.* at § 8.4(2)(b).

However, the original electronic devices should only be transmitted when necessary for the subject matter assistance.[102] When a Special Agent determines there is probable cause of unlawful activity after reviewing information searched during a border search, the Special Agent may seize and retain both the device and the information.[103] All retained information from electronic devices determined to be of no relevance to ICE will be destroyed within seven business days after the conclusion of the border search unless circumstances require more time.[104] All destructions must be accomplished no later than 21 calendar days after conclusion of the search.[105]

According to the Directive, "all electronic devices crossing U.S. borders are subject to border search," and a claim of privilege or personal information will not prevent the search. However, certain types of information are subject to special handling by ICE Special Agents.[106] Business or commercial information is to be treated as business confidential information.[107] Legal information and other information claimed to be protected by attorney-client or attorney work privilege can be searched if the Special Agent suspects that the content of the information constitutes evidence of a crime or some other matter that falls within the jurisdiction of ICE. In such a case, the Special Agent must consult the ICE Office of the Chief Counsel or the appropriate U.S. Attorney's Office before beginning the search. Other sensitive information, such as medical records or journalist work-related information will be handled pursuant to federal law and ICE policy, and questions regarding such review, shall be directed to the ICE Office of the Chief Counsel.

Conclusion

It is arguable that there is a higher expectation of privacy surrounding the contents of laptops than other types of physical property, such as vehicle interiors. Even when a vehicle search involves an onerous and time-consuming inspection of a gasoline tank, some would argue that the expectation of privacy surrounding the vehicle and its contents does not appear to be as high as the expectation of privacy regarding the contents of a laptop, which often contains private thoughts or other forms of privileged information. On the other hand, laptop searches are not considered by the courts as intrusive as strip or body-cavity searches, where the expectation of privacy surrounding one's body is considered higher.[108] Although the Ninth Circuit in *Arnold* has analogized laptop searches to all other searches of personalty, other federal circuits may agree with Judge Kozinski in holding that the government owes greater deference to the privacy interest surrounding laptops.

In addition to privacy interests, courts have taken a range of other concerns into account when determining whether reasonable suspicion must justify a warrantless border search. For example, when courts have conducted border search analyses, they have frequently considered potential harms resulting from illegal materials smuggled into the United States through laptops and electronic storage devices. As stated in *Ramsey*, "The border search exception is grounded in the

[102] *Id.* at § 8.4(4).

[103] *Id.* at § 8.5(1)(a).

[104] *Id.* at § 8.5(1)(e).

[105] *Id.*

[106] *Id.* at § 8.6(1).

[107] *Id.* at § 8.6(2)(a).

[108] *Chase*, 503 F.2d 571 (strip searches require reasonable suspicion); *Montoya de Hernandez*, 473 U.S. 531 (alimentary canal search justified by reasonable suspicion).

recognized right of the sovereign to control ... who and what may enter the country."[109] Laptops can present a challenge to the nation's ability to control what enters its borders because the vast and compact storage capacity of laptops can be used to smuggle illegal materials. In light of this, courts have held that routine searches of laptops at the border may be justified because of the strong government interest in preventing the dissemination of child pornography and other forms of "obscene" material that may be contained in laptops.[110] Another justification may be to facilitate searches of laptops owned by suspected terrorists, which may contain information related to a planned terrorist attack.[111]

On the other hand, if customs officials can conduct laptop border searches without the need for reasonable suspicion, there is the potential for customs officials to conduct targeted searches based on justifications prohibited by the Constitution. For example, if a customs official could conduct a search without cause, it may be more difficult to detect unlawful bases for the searches because the official would not need to explain why he conducted the search. Such concerns suggest that resolving the issues surrounding laptop border searches will involve striking a careful balance between national security and civil liberties.

The Ninth Circuit, by equating the privacy interest implicated in personal information with that surrounding normal personal effects, has adopted a categorical approach to the border search doctrine. The court has concluded that the search of all personal property does not require reasonable suspicion unless the search is conducted in a manner that is destructive or particularly offensive.[112] So far, the Ninth Circuit is the only circuit to have explicitly stated that such searches do not require reasonable suspicion. Whether other federal circuits adopt this approach or, in the same vein as Judge Kozinksi, give credence to the notion that a heightened expectation of privacy surrounds expressive materials, thus requiring reasonable suspicion before being searched, is an open question.

Legislative Proposals

A bill introduced in the 111th Congress, the Securing our Borders and our Data Act of 2009 (H.R. 239), would prohibit laptop searches based solely on border search authority.[113] The legislation would establish "fundamental rules" prohibiting a federal border officer from searching or seizing a "digital electronic device" or "electronic storage media" based solely on the power of the United States to search and seize the effects of individuals seeking entry into the country. Instead, the legislation would allow such searches only in cases where border officers have reasonable suspicion that a device contains criminal evidence. Devices could be seized only if constitutional authority other than border search authority provided a justification. The bill would direct the Secretary of Homeland Security to promulgate rules regarding: maximum time periods during which border officers can detain devices; owners' rights to retrieve detained devices; and

[109] *Ramsey*, 431 U.S. at 611.

[110] *See, e.g.*, New York v. Ferber, 458 U.S. 747, 765 (1982) (holding that child pornography does not enjoy First Amendment protections because the government has a compelling state interest in preventing the sexual abuse of children and that the distribution of child pornography is intrinsically related to that state interest).

[111] *See Ickes*, 393 F.3d at 506.

[112] *Arnold*, 533 F.3d at 1007-1008.

[113] The Securing our Borders and our Data Act of 2009, H.R. 239, 111th Cong. (2009).

strategies for maintaining the integrity of all information detained and shared with other government agencies.[114]

The Border Security Search Accountability Act of 2009 (H.R. 1726) would mandate that the Commissioner of Customs and Border Protection promulgate a rule with respect to the scope of procedural and record-keeping requirements associated with border security searches of electronic devices.[115] The rule would require that commercial information be handled in a manner consistent with all laws and regulations governing such information, that electronic searches be conducted in front of a supervisor, that a determination of the number of days such information could be retained without probable cause be made, that the individual whose information was seized be notified if the information is entered into an electronic database, that an individual receive a receipt if his device is seized during a border search, that an individual subject to a border search of an electronic device receive notice as to how he can report any abuses or concerns related to the search, that the rights of individuals with regard to border searches be posted at all ports of entry, that a privacy impact assessment of the rule be made, and that a civil rights impact assessment of the rule be made.[116]

Author Contact Information

Yule Kim
Legislative Attorney
ykim@crs.loc.gov, 7-9138

[114] This legislation is identical to a bill introduced during the 110th Congress. *See* Securing Our Borders and Our Data Act of 2008, H.R. 6702, 110th Cong. (2008). Another related bill introduced during the 110th Congress, H.R. 6588, would have prohibited laptop searches based on the United States' border search authority but permitted laptop searches conducted under any other federal authority. *See* Electronic Device Privacy Act of 2008, H.R. 6588, 110th Cong. (2008).

[115] Border Security Search Accountability Act of 2009, H.R. 1726, 111th Cong. (2009).

[116] This bill is similar to H.R. 6869, introduced in the 110th Congress, which would have directed the Department of Homeland Security to issue rules regarding the scope and procedural requirements associated with border security searches of electronic devices. *See* Border Security Search Accountability Act of 2008, H.R. 6869, 110th Cong. (2008).