PAUL HASTINGS

STAY CURRENT

March 2017

Follow @Paul_Hastings

International Travelers Beware–Digital Device Searches at the Border

By Behnam Dayanim & Ashley Pyon

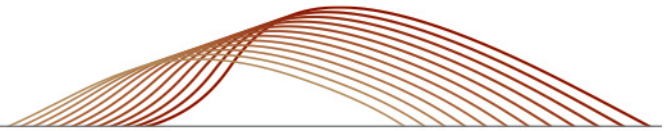
International travelers traveling with electronic devices beware. In recent years, the number of electronic media searches at U.S. borders has increased dramatically. In fiscal year 2016, 390 million people entered the U.S., and 23,877 electronic media searches were conducted at the border. In fiscal year 2015 there were only 4,764.[1] And under the Trump Administration, that number is likely to grow. Last month, in a Q&A with the House Homeland Security Committee, Secretary John Kelly identified as a "glaring deficiency" what he termed as the previous administration's reluctance to scrutinize immigrants' social networking accounts during their vetting processes.[2] Moreover, in light of the recent executive order on terrorism and immigration, travelers, including attorneys, who may be carrying sensitive privileged information, should be increasingly aware of their rights at the border—or lack thereof.

This article provides an overview of (1) the U.S. Customs and Border Protection ("CBP") authority to conduct searches at the border, (2) the evolving approach courts have adopted toward digital border searches, and (3) the rights of attorneys—including non-U.S. attorneys—at the border to assert attorney-client privilege. This article also provides recommendations as to what U.S. citizens and attorneys can do to protect their personal information.

I. Border Searches Are an Exception to the Fourth Amendment's Probable Cause and Warrant Requirements

The Fourth Amendment to the United States Constitution protects individuals against unreasonable government searches and seizures.[3] However, border searches are recognized as a long established exception to the Fourth Amendment's probable cause and warrant requirements. The Supreme Court has said, "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border . . ."[4] Moreover, the Court has held that routine border searches may be conducted without a search warrant, even in the absence of reasonable suspicion because "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the International border."[5]

Warrantless searches are conducted by federal law enforcement agencies, including CBP and the U.S. Immigration and Customs Enforcement ("ICE"), and are authorized by statute. Title 19 U.S.C.§ 1582 authorizes "the search of persons and baggage" and provides that "all persons coming into the United States from a foreign country shall be liable to detention and search by authorized



officers or agents of the Government under such regulations."[6] 19 C.F.R. 162.6 further describes CBP's authority to conduct border searches, which provides that "[a]ll persons, baggage and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection by a CBP officer."[7] Additionally, the courts have repeatedly found that suspicion is not required for a routine border search.[8]

II. Digital Searches at the Border

In today's digital era, courts have grappled with growing legal issues surrounding the search of electronic devices at the border, particularly whether such searches would be viewed as routine or nonroutine and whether reasonable suspicion is required. In recent years, courts have increasingly required "reasonable suspicion" due to the intrusiveness of digital searches.

The U.S. Court of Appeals for the Ninth Circuit's decision in *United States v. Cotterman* exemplifies courts' recent moves toward requiring reasonable suspicion.[9] The court in *Cotterman* held that a search of the defendant's computer at the border was a forensic digital search and therefore nonroutine, requiring reasonable suspicion.[10] The court emphasized that the technological capabilities of modern cell phones and laptops make a forensic digital search especially intrusive—and analytically distinct from searches of other forms of property.[11] This decision departed from the Ninth Circuit's previous decision in *United States v. Arnold*, in which the court found that laptop searches by airport customs officials to be routine and not requiring reasonable suspicion.[12] The court distinguished *Cotterman* from *Arnold* by concluding that while "routine cursory inspections," as was the case in *Arnold*, would have been reasonable without particularized suspicion, the forensic search in *Cotterman* was unreasonable because the agents proceeded to comprehensively analyze hard drives, which was "essentially a computer strip search."[13]

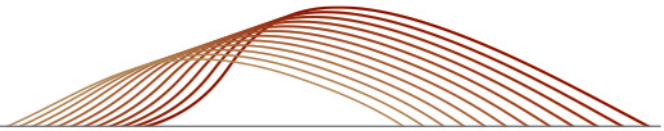
Cotterman also represents a shift from the Fourth Circuit's holding in *United States v. Ickes*, in which the court reasoned that computer searches were routine because computer files were indistinguishable from any other "cargo" subject to routine search and inspection at the border. Contrary to the holding in *Ickes*, *Cotterman* distinguished forensic searches of electronic devices from physical belongings by finding that forensic searches are quantitatively and qualitatively different from routine border searches of physical belongings.[14]

The recent Supreme Court decision in *Riley v. California*[15] provides further insight as to how courts may view digital searches.

The Court ruled that "a warrant is generally required" before searching information stored on a cell phone seized incident to an arrest. Although the Riley case did not involve a border search, the Court's conclusion that digital searches are inherently more intrusive than searches of physical objects—such as briefcases or notebooks—carries implications in the border context as well. Importantly, the Riley Court based its holding not on the nature of the data reviewed or the manner of the review, but instead on the fact that digital devices contain a vast quantity of data that are qualitatively and quantitatively different from what is typically found in other, analog objects.[16]

Although *Riley* did not involve a border search, at least one court has applied the decision in rejecting the search of a laptop "as supported by so little suspicion of ongoing or imminent criminal activity, and . . . so invasive of [defendant's] privacy," that it was unreasonable.[17]

Riley suggests that courts should treat searches of digital media differently from routine border examinations, which would point toward a "reasonable suspicion" requirement. However, that is not



settled law, and, regardless of the test employed, the risk presented to confidential information stored in digital devices remains substantially higher at the border than in a wholly domestic context.

III. Attorney-Client Privilege at the Border

Border searches of lawyers carrying client confidential information raises unique privilege concerns. Although there appear to be no cases discussing privileged material in the context of an electronic border search, *Looper v. Morgan* addressed traditional searches of attorneys' paper files at the border. The court in *Looper* held that privileged documents should be returned without the possibility of inspection, stating that "when a Customs official, in the course of a routine border search, seeks to take the nonroutine step of reading the contents of any document over an attorney's objection that the document is privileged, Customs may not read the document without a warrant or subpoena."[18]

Despite courts' recognition of attorney-client privilege at the border, CBP does not categorically exclude privileged materials from searches. The U.S. Customs and Border Protection Policy states that "[a]lthough legal materials are not necessarily exempt from a border search, they may be subject to special handling procedures. Correspondence, court documents, and other legal documents may be covered by attorney-client privilege. If an officer suspects that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP, the officer must seek advice from the Associate/Assistant Chief Counsel or the appropriate U.S. Attorney's office before conducting a search of the document."[19] Additionally, CBP has imposed a time frame of five days for returning a device; however, this can be extended for up to 30 days.[20]

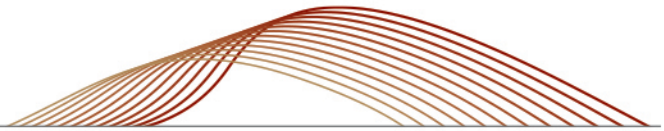
IV. Foreign Attorneys May Assert Attorney-Client Privilege

International matters often involve both U.S. and foreign attorneys, and U.S. companies and law firms increasingly maintain non-U.S. legal offices or outsource legal work to countries outside the United States. In addressing those scenarios, many courts have adopted a "touch base" approach to determine whether to extend U.S. attorney-client privilege to foreign attorneys. Using this approach, the court first decides whether the communication involves U.S. or foreign law and then reviews that applicable privilege law. U.S. law, and subsequently the extension of attorney-client privilege, governs communications involving U.S. issues; foreign law governs communications relating to matters solely involving foreign jurisdictions. The jurisdiction with the predominant interest is the location where the privileged relationship took place or the location in which that relationship was centered when the communication took place, unless application of foreign law would be contrary to the public policy of the forum.[21] This means that if a foreign attorney is representing a U.S. client, or has privileged material involving a U.S. matter, courts will often extend attorney-client privilege to that attorney and his or her files.

V. Recommendations for Travelers and Attorneys at the Border

Encrypt everything. Evolving case law illustrates that courts are increasingly finding digital searches to be nonroutine, thereby requiring reasonable suspicion. The harder it is for a border official to extract data, the more intrusive the search becomes and the more likely it will be considered nonroutine and subject to a heightened threshold.[22]

For attorneys targeted by border officials, the best course of action is to claim privilege clearly, loudly, and as soon as possible. It may be best practice to have a print-out of CBP's published practices available to show border officials who may not be aware of the CBP's special handling procedures for attorney-client privileged material.



Lastly, consider not bringing anything sensitive. If you do not have it, the government cannot get it.

If you have any questions regarding the rule or compliance with the new requirements, please contact a member of our Privacy & Cybersecurity Practice.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

New York

James H. Koenig
1.212.318.6005
jimkoenig@paulhastings.com

Thomas A. Counts
1.415.856.7077
tomcounts@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

San Francisco

Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Ashley J. Pyon
1.202.551.1884
ashleypyon@paulhastings.com

---

[1] *See* Tal Kopan, First on CNN: Senator Seeks Answers on Border Cell Phone Searches, CNN, Feb.20, 2017, *available at* http://www.cnn.com/2017/02/20/politics/border-search-cell-phones-ron-wyden-dhs-letter/.

[2] *See* Border Security and Immigration Enforcement, Part 1, C-SPAN, Feb 7, 2017, *available at* https://www.c-span.org/video/?423321-1/homeland-security-secretary-john-kelly-testifies-us-border-security.

[3] U.S. CONST. AMEND. IV.

[4] *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

[5] *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004).

[6] 19 U.S.C. § 1582; *see also* 19 U.S.C. § 482 (authorizing the search of vehicles and persons regarding merchandise); 19 U.S.C. § 1467 (special inspection, examination and search); 19 U.S.C. § 1496 (authorizing the examination of baggage); 19 U.S.C. § 1499 (authorizing the examination of merchandise); 19 U.S.C. § 1581 (authorizing the boarding of vessels/searching of vehicles). *See generally* 8 U.S.C. § 1357(c) (granting the authority to board and search any conveyance believed to be bringing aliens into the United States); 8 U.S.C. § 1225(d)(1) (granting immigration officers the authority to board and search any conveyance believed to be bringing aliens into the United States).

[7] 19 C.F.R. 162.6.

[8] *U.S. v. Ross*, 456 U.S. 798, 823 (1982) (holding a customs officer may randomly search luggage carried by a traveler no matter the traveler's desire to conceal the contents); *Torres v. Puerto Rico*, 442 U.S. 465, 472-73 (1979) (stating that "[t]he authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity); *U.S. v. Ramsey*, 431 U.S. 606, 616 (1977) ("searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border . . .").

[9] *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013).

[10] *Id.* (concluding that "the comprehensive and intrusive nature of a forensic examination—not the location of the examination," requires that there be a reasonable suspicion to support the warrantless search under the Fourth Amendment).

[11] *Id*. at 965.

[12] *United States v. Arnold*, 533 F.3d 1003, 1008 (9th Cir. 2008).

[13] *Id*. at 966.

[14] *Id*. at 960; *See also United States v. Saboonchi*, 990 F. Supp. 2d 536 (D. Md. 2014) (finding that the search of two smartphones and flash drives constituted a forensic search because it was intrusive and therefore nonroutine and required reasonable suspicion).

[15] *Riley v. California*, 134 S. Ct. 2473, 2493 (2014).

[16] *Riley*, 134 S. Ct. at 2481.

[17] *United States v. Kim*, 103 F. Supp.3d 32, 58 (D.D.C., 2015).

[18] *Looper v. Morgan*, No. H-92-0294, 1995 U.S. Dist. LEXIS 10241, *16 (S.D. Tex. June 30, 1995).

[19] *See* U.S. Customs and Border Protection Policy Regarding Border Search of Information (July 16, 2008), *available at* https://www.cbp.gov/sites/default/files/documents/search_authority_2.pdf.

[20] *See* Mary Ellen Callahan, *Privacy Issues In Border Searches of Electronic Devices* (October 2009), *available at* https://www.dhs.gov/sites/default/files/publications/privacy_privacy_issues_border_searches_electronic_devices.pdf.

[21] *Wultz v. Bank of China Ltd*., 979 F. Supp. 2d 479, 488–92 (S.D. N.Y. 2013), on reconsideration in part, 2013 WL 6098484, *2 (S.D. N.Y. 2013) (applying the "touch base" approach and finding that Chinese law, which applied to communications that occurred entirely in China and did not relate to U.S. legal matters, would not protect communications with counsel from disclosure); *Kiobel v. Royal Dutch Petroleum Co*., 2005 WL 1925656, *2 (S.D. N.Y. 2005); *Astra Aktiebolag v. Andrx Pharmaceuticals, Inc*., 208 F.R.D. 92, 98 (S.D. N.Y. 2002); *Chubb Integrated Systems Ltd. v. National Bank of Washington*, 103 F.R.D. 52, 65, 39 Fed. R. Serv. 2d 1262 (D.D.C. 1984) (applying the "touch base" test but declining to extend the attorney-client privilege to foreign patent agents).

[22] *See In re Grand Jury Subpoena Duces Tecum* (holding that a subpoenaed individual's act of decrypting and producing for the grand jury the contents of hard drives seized during the course of a child pornography investigation was sufficiently testimonial to trigger Fifth Amendment protection).