Protecting Your Digital Devices at the Border

A Criminal Defense Lawyer's Primer

October 2017

Courts have long made it clear that agents can search the bags of people entering the country. For the past decade or so, U.S. Customs and Border Protection (CBP) has applied that logic to digital devices. NACDL members are uniquely exposed to abuse in this context: digital devices store materials and information subject to the attorney-client privilege and attorney work-product doctrine, as well as information on overseas clients and witnesses, and other extremely sensitive materials that could be covered by Rule 1.6 of the Model Rules of Professional Responsibility.

What does CBP think it can do?

CBP asserts that it can search people crossing the border (*i.e.*, at a land crossing or other port of entry) without a warrant and without suspicion.[1] The courts have established that Fourth Amendment rights are limited at the border in the name of national security.[2] CBP extends that search authority to digital devices pursuant to a 2008 CBP guidance and 2009 CBP directive.[3]

The courts refer to a search of a traveler's person and possessions as a "routine search." Agents conducting routine searches do not need a warrant or reasonable suspicion.[4]

Manual searches of digital devices require little technical knowledge—they usually involve flipping through digital files, images, or browser history.[5] Forensic searches tend to depend on technical experts who can use sophisticated technology to probe a device.[6] In the Ninth Circuit, border agents need reasonable suspicion to conduct a forensic search, but none at all for a manual search.[7]

Under CBP policy, if agents seize a device at the border, further actions are considered part of that original search. A digital device seized at the border may be sent to another agency or moved to a completely different physical location, all as a part of a single border search.[8]

---

[1] *See* Office of Senator Ron Wyden, *Due Diligence Questions for Kevin McAleenan* (June 20, 2017) at 1 (Describing the statutory authority for border searches, "…e.g., 8 US.C. §1357; 19 US.C. §§ 1461, 1499; see also 19 C.F.R. § 162.6, stating that '[a]ll 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.'").

[2] The border search exception holds that the government's agency to protect its interests at the border generally outweighs any individual traveler's privacy rights. *See* Sophia Cope et al., *Digital Privacy and the U.S. Border: Protecting the Data on Your Devices and the Cloud*, Electronic Frontier Foundation (2017), at 24 n. 24.

[3] U.S. Customs and Border Protection, Policy Regarding Border Search of Information (July 16, 2008); U.S. Customs and Border Protection, CBP Directive No. 3340-049 (Aug. 20, 2009).

[4] *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985) at 538 ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant…").

[5] *See, e.g.*, *Abidor v. Napolitano*, 990 F.Supp.2d 260 (E.D.N.Y. 2013) at 260-270 ("A quick look entails only a cursory search that an officer may perform manually. It involves opening the computer and viewing the computer's contents as any lay person might be capable of doing simply by clicking through various folders.").

[6] Sophia Cope et al., *supra* note 2, at 43, 48.

[7] *United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013) (Given that "[a]n exhaustive forensic search of a copied laptop hard drive intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border.").

[8] U.S. Customs and Border Protection, *supra* note 3 at 4-5.

CBP treats data stored on devices and data stored externally in different ways. According to a letter from acting CBP Commissioner Kevin McAleenan, the agency may not access externally stored data, *i.e.*, data resident on servers or cloud storage, in the course of a routine border search.[9] McAleenan, writing in response to queries from Senator Ron Wyden, maintains that agents may search any information that is stored on devices. As of August 2017, CBP has not released the guidance relevant to Wyden's questions, nor has any such document been acquired through FOIA.

In September 2017, the ACLU and EFF filed suit in the District Court of Massachusetts on behalf of eleven plaintiffs to challenge these practices. The lawsuit alleges Fourth and First Amendment violations and seeks to establish a warrant requirement for such searches.[10]

What rights do you have at the border?

Any traveler can refuse to comply with a border search of a digital device. Of course, doing so will have significantly different meaning depending on a person's citizenship status.

Border agents cannot deny entry to a U.S. citizen who declines to unlock a device or provide passwords. CBP can, and often does, subject citizens who do so to intensive questioning. Agents can coercively detain a citizen who refuses to comply with a device search. For instance, one of the plaintiffs in the ACLU suit reports that the search of his device took two hours, during which he remained in CBP custody with agents acting in a threatening manner.[11] Non-citizens who decline to comply may be denied entry into the country, while lawful permanent residents may see their status endangered.[12]

How do border agents treat attorneys?

CBP does not guarantee protection for privileged communications at the border. NACDL members who joined a suit challenging digital searches report "serious ethical dilemmas" about traveling overseas, given that work trips might result in the disclosure of information about their clients.[13] Indeed, Rule 1.6 of the Model Rules of Professional Conduct establishes that "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent."[14] Thus, Rule 1.6 is broader than the attorney-client privilege.[15]

---

[9] Office of Senator Ron Wyden, *supra* note 1 at 3 (stating that "[i]n conducting a border search, CBP does not access information found only on remote servers through an electronic device presented for examination, regardless of whether those servers are located abroad or domestically. Instead, border searches of electronic devices apply to information that is physically resident on the device during a CBP inspection.").
[10] Complaint, *Alasaad v. Duke*, No. 17-cv-11730 (D. Mass.).
[11] *Id*. at 24.
[12] Sophia Cope et al., *supra* note 2 at 9.
[13] Complaint at 20, *Abidor v. Napolitano*, 990 F.Supp.2d 260 (E.D.N.Y. 2013).
[14] Model Rules of Prof'l Conduct R. 1.6 (2012).
[15] *See*, for an extended treatment of Rule 1.6's relevance, The Association of the Bar of the City of New York, *Formal Opinion 2017-5: An Attorney's Ethical Duties Regarding U.S. Border Searches of Electronic Devices Containing Clients' Confidential Information* (July 25, 2017), *available at* http://s3.amazonaws.com/documents.nycbar.org/files/2017-5_Border_Search_Opinion_PROETHICS_7.24.17.pdf.

CBP provides guidance for agents who search attorneys, but it does not provide much clarity on the degree of protection attorneys can expect for client information:

> Officers may encounter materials that appear to be legal in nature, or an individual may assert that certain information is protected by attorney-client or attorney work-product privilege. Legal materials are not necessarily exempt from a border search, but they may be subject to the following special handling procedures: If an Officer suspects that the content of such a material may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP, the Officer must seek advice from the CBP Associate/Assistant Chief Counsel before conducting a search of the material, and this consultation shall be noted in appropriate CBP systems of records. CBP counsel will coordinate with the U.S. Attorney's Office as appropriate.[16]

It is not clear what "seek advice" constitutes, nor if the CBP counsel who is consulted may recommend that a search not take place at all. In any event, CBP policy fails to acknowledge that neither the attorney-client privilege, the attorney work-product doctrine, nor Rule 1.6 are limited to "material [that] may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP[.]" Those confidential aspects of an attorney's communications and files do not depend on the existence of litigation at all, and in fact are far more voluminous in the non-litigation context.

What steps can you take?

The courts have yet to address the border searches of digital devices that contain information subject to attorney-client privilege or attorney work-product doctrine. Though the steps detailed below are as yet untested, we encourage NACDL members to be proactive.

- The Second Circuit case *U.S. v. Kovel* held that confidential communications between a client and an accountant hired by a law firm specifically for the purpose of legal advice functioned under attorney-client privileges.[17] Practitioners of tax law often use so-called *Kovel* letters to ensure that outside experts can engage in privileged communications, though under a number of specific limitations.[18] *Kovel* letters might be used to ensure that investigators traveling overseas can assert attorney-client privilege at the border.

- A court may grant a protective order under Rule 16(d) of the Federal Rules of Criminal Procedure.[19] The potential for the violation of attorney-client privilege or work-product privilege at the border may constitute good cause for a judge to issue a protective order for a digital device.

---

[16] U.S. Customs and Border Protection, Policy Regarding Border Search of Information, *supra* note 3 at 3. *Compare* U.S. Customs and Border Protection, CBP Directive No. 3340-049, *supra* note 3 at 4.
[17] *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961).
[18] *See* Martin A. Schainbaum, *The Scope and Limitations of the Kovel Accountant*, The Champion (March 2016), *available at* https://www.nacdl.org/Champion.aspx?id=40997.
[19] Fed. R. Crim. P. 16(d).

- A person being searched or detained by CPB will not be able to communicate to the outside world. One option to ensure some degree of protection for traveling attorneys is to arrange a "buddy system": arrange for another lawyer to appear at a port of entry if the traveler does not make contact within a given time span after arrival. The second lawyer can act as a monitor in case the traveler is detained. The traveling attorney (or other person) and the monitoring lawyer should file a DHS Form G-28, "Notice of Entry of Appearance as Attorney or Accredited Representative," prior to travel in order to ensure the monitoring attorney's access and ability to intervene.[20] While a Power of Attorney can serve a similar purpose, the G-28 is the more formal and recognized method.

- Attorneys who are traveling may benefit from a small card printed with the text of Rule 1.6 of the Model Rules of Professional Conduct to show to CPB agents.

Device owners can take a number of technological steps in order protect their devices. Encryption technologies can make your data hard to access without certain passwords, while cloud-based storage can ensure that no sensitive data resides on your device. Devices can also be rented for specific trips in order to reduce the volume of data to which CBP might gain access through a search or seizure of a device. Please reference a technology-specific guide to understand what you can do.

Resources

Complaint in *Alasaad v. Duke* (https://www.aclu.org/sites/default/files/field_document/alasaad_v._duke_complaint_2.pdf)

Electronic Frontier Foundation, "Digital Privacy and the U.S. Border: Protecting the Data on Your Devices and the Cloud" (https://www.eff.org/files/2017/03/10/digital-privacy-border-2017-guide3.10.17.pdf)

Office of Senator Ron Wyden, Due Diligence Questions for Kevin McAleenan (http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/170712-cpb-wyden-letter.pdf)

U.S. Customs and Border Protection, Policy Regarding Border Search of Information (2008) (https://www.cbp.gov/sites/default/files/documents/search_authority_2.pdf)

U.S. Customs and Border Protection, CBP Directive No. 3340-049 (2009) (https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf)

U.S. Department of Homeland Security, Notice of Entry of Appearance as Attorney or Accredited Representative (https://www.uscis.gov/sites/default/files/files/form/g-28.pdf)

Wired, "A Guide to Getting Past Customs with Your Digital Privacy Intact" (https://www.wired.com/2017/02/guide-getting-past-customs-digital-privacy-intact/)

[20] U.S. Department of Homeland Security, Notice of Entry of Appearance as Attorney or Accredited Representative.