Linda A. Klein
President

AMERICAN BAR ASSOCIATION

321 North Clark Street
Chicago, IL 60654-7598
(312) 988-5109
Fax: (312) 988-5100
abapresident@americanbar.org

Defending Liberty
Pursuing Justice

May 5, 2017

General John F. Kelly, USMC (Ret.)
Secretary of Homeland Security
Office of the Secretary
Department of Homeland Security
Washington, D.C. 20528

Joseph B. Maher
Acting General Counsel
Office of the General Counsel
Department of Homeland Security
Washington, D.C. 20528

Re: Preservation of Attorney-Client Privilege and Client Confidentiality for U.S. Lawyers and Their Clients During Border Searches of Electronic Devices

Dear General Kelly and Mr. Maher:

On behalf of the American Bar Association ("ABA"), which has over 400,000 members, I write to express our serious concerns regarding the standards that permit U.S. Customs and Border Protection ("CBP") and Immigration and Customs Enforcement ("ICE") officers to search and review the content of lawyers' laptop computers, cell phones, and other electronic devices at U.S. border crossings without any showing of reasonable suspicion. These devices typically contain client information that is inherently privileged or otherwise confidential. As ABA President, I have been contacted by our members who have expressed concern about maintaining the confidentiality of client information contained in lawyers' electronic devices when re-entering the United States. I share these concerns and urge you to ensure that the proper policies and procedures are in place at the Department of Homeland Security ("DHS"), CBP, and ICE to preserve the attorney-client privilege, the work product doctrine, and the confidentiality of lawyer and client communications during border crossings and to prevent the erosion of these important legal principles.

The ABA understands and supports the critical role that DHS, CBP, and ICE play in protecting our national security. We recognize that security at the nation's borders is of fundamental importance, and we acknowledge that lawyers traveling across the border with laptops and other electronic devices containing confidential client documents and other information could become subject to routine searches by CBP and ICE agents. But just as border security is fundamental to national security, so too is the principle of client confidentiality fundamental to the American legal system.

A cornerstone of our legal system—both civil and criminal—is the confidential lawyer-client relationship, which includes the lawyer's strict ethical duty to preserve the confidentiality of communications with the client. *See Upjohn Co. v. United States,* 449 U.S. 383 (1981). ABA Model Rule of Professional Conduct 1.6(a) states in pertinent part that "a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent …." (*See* ABA Model Rule of Professional Conduct 1.6, and the related commentary, available at http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html. *See also* Charts Comparing Individual Professional Conduct Rules as Adopted or Proposed by States to ABA Model Rules, available at http://www.americanbar.org/groups/professional_responsibility/policy.html.)

The lawyer's duty to preserve client confidentiality is broad and encompasses material that is protected by the attorney-client privilege and the work product doctrine, as well as any other non-privileged information that the client wishes to keep confidential. The attorney-client privilege and client confidentiality enable clients to communicate with their lawyers in confidence, which is essential to preserving the clients' right to effective counsel. Protecting confidential communications between clients and lawyers also encourages clients to seek out and obtain guidance to conform their conduct to the law, facilitates self-investigation into past conduct to identify shortcomings and remedy problems, and enables lawyers to fulfill their ethical duties to their clients, all of which benefit society at large. The work product doctrine underpins our adversarial justice system and allows attorneys to prepare for litigation without fear that their work product and mental impressions will be revealed to adversaries, to the detriment of their clients.

The ABA has consistently fought to preserve the attorney-client privilege, the work product doctrine, and the confidential lawyer-client relationship. For example, the ABA recently worked with the then-Director and General Counsel of the National Security Agency ("NSA") and other federal agencies to ensure that their "minimization procedures" protect the confidentiality and attorney-client privileged status of lawyer-client communications intercepted or otherwise received by the NSA or other agencies. (*See* the ABA's February 2014 letter to the NSA, available at http://www.americanbar.org/content/dam/aba/uncategorized/GAO/2014feb20_nsainterceptionofprivilegedinfo_l.authcheckdam.pdf and the NSA's March 2014 response letter, available at http://www.americanbar.org/content/dam/aba/uncategorized/GAO/2014mar10_interceptionofprivilegedinfo_nsaresponse.pdf.)

The same concerns that prompted ABA communication and collaboration with the NSA lead us now to urge DHS to clarify key provisions of the CBP and ICE policies governing searches of lawyers' and other travelers' electronic devices at the U.S. border. In particular, we urge you to clarify Section 5.2 of the CBP Directive No. 3340-049 ("Border Search of Electronic Devices Containing Information," dated August 20, 2009) and Sections 6.1 and 8.6 of the ICE Directive No. 7-6.1 ("Border Searches of Electronic Devices," dated August 18, 2009). The CBP Directive is available at https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf, and the ICE Directive is available at https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf).

Both the CBP and ICE Directives have resulted in CBP Officers and ICE Special Agents exercising sweeping powers to search electronic devices at the border, with or without reasonable suspicion of any wrongdoing. Such activities could expose those officers and agents to allegations of misconduct or overreaching due to the ambiguity of the language in the directives. In particular, Section 5.1.2 of the CBP Directive states that "in the course of a border search, with or without individualized suspicion, an Officer may examine electronic devices and may review and analyze the information...", subject to the requirements and limitations in the Directive and applicable law. Sections 5.2 to 5.4 of the CBP Directive allows Officers to review, detain, seize, and retain electronic devices and information and to share that information with other agencies.

Similarly, Section 6.1 of the ICE Directive states 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, consistent with the guidelines and applicable laws set forth herein." Section 8.6(1) of the ICE Directive further provides that "all

electronic devices crossing U.S. borders are subject to border search..." and that while "a claim of privilege or personal information does not prevent" such a search, "the nature of certain types of information are subject to special handling by Special Agents, whether through policy or laws such as the Privacy Act and the Trade Secrets Act."

These broad claims of authority in the CBP and ICE Directives are limited somewhat by other provisions that require special review and handling of privileged or sensitive materials. In particular, both Section 5.2.1 of the CBP Directive and Section 8.6(2)(b) of the ICE Directive require that when (1) material appears to be "legal in nature" or an individual asserts that certain material is protected by "the attorney-client or attorney work product privilege" and (2) the officer or agent suspects that the content of the material may "constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction" of CBP or ICE, the officer or agent must consult with the CBP Associate/Assistant Chief Counsel, the ICE Office of the Chief Counsel, or the appropriate U.S. Attorney's Office before conducting a search of the material. Section 5.2.4 of the CBP Directive further provides that information that is determined to be privileged or sensitive "will only be shared with federal agencies that have mechanisms in place to protect appropriately such information."

While we appreciate the CBP and ICE Directives' acknowledgement that privileged and confidential legal materials should be accorded "special handling" during border searches, we are concerned that these key provisions outlined above are not sufficiently clear or comprehensive enough to protect these fundamental legal rights.

Courts have generally permitted routine cursory border searches of travelers' computers and other electronic devices as an exception to the Fourth Amendment prohibition against warrantless searches without probable cause. *See, e.g., U.S. v. Cotterman*, 709 F.3d 952, 960-961 (9th Cir. 2013) (en banc) and *Abidor v. Napolitano*, 990 F. Supp.2d 260, 277-282 (E.D.N.Y. 2013). However, the Ninth Circuit has also concluded that an intrusive forensic search of a computer hard drive is not "routine" and hence requires reasonable suspicion to be permissible. S*ee Cotterman,* 709 F.3d at 960-968 (holding that while a "quick look and unintrusive search of laptops" at the border is generally permissible without any showing of cause, an extensive forensic search is "essentially a computer strip search" and requires a showing of reasonable suspicion to be lawful).

In addition, at least one federal court has held that "the reading, duplication, or seizure of documents claimed to be privileged, over the objection of the attorney transporting them, is also a form of 'nonroutine' border search." *See Looper v. Morgan,* Civ. No. H-92-0294, 1995 U.S. Dist. LEXIS 10241 (S.D. Tex. June 23, 1995). That court also concluded 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."

We know that DHS, CBP, and ICE, as federal agencies committed to the rule of law, recognize the importance of preserving the attorney-client privilege, the work product doctrine, client confidentiality, and the right to effective counsel. Therefore, we respectfully request that you revise the CBP and ICE Directives in several specific ways.

First, we urge you to modify and clarify Section 5.2 of the CBP Directive and Section 8.6 of the ICE Directive to emphasize and protect these fundamental legal rights and provide your front line agents and officers with explicit guidance as to the importance of these principles. Specifically, Sections 5.2 and 8.6 should be revised to state that when a lawyer traveling across the border with a laptop computer or other electronic device asserts that the device contains privileged or confidential client information, the device can be subjected only to a routine cursory physical inspection. In addition, Sections 5.2 and 8.6 should specifically state that the privileged or confidential electronic documents and files on the device cannot be read, duplicated, seized, or shared unless the CBP Officer or ICE Special Agent first obtains a subpoena based on reasonable suspicion or a warrant supported by probable cause.

Second, we urge you to revise these Directives to clarify the specific standards and procedures that CBP and ICE agents must follow before the contents of a lawyer's electronic device can be searched or seized at the border. Specifically, we recommend that DHS clarify Section 5.2 of the CBP Directive and Section 8.6 of the ICE Directive to:

(1) provide a clear standard that a CBP Officer or ICE Special Agent must follow prior to demanding a search or seizure of the documents and files on a lawyer's electronic device;

(2) indicate what conduct is expected of the CBP Officer or ICE Special Agent when a lawyer asserts that an electronic device contains confidential client information protected under the attorney-client privilege, the work product doctrine, or the applicable rules of professional conduct; and

(3) define specifically when the CBP Officer or ICE Special Agent must consult with the CBP Associate/Assistant Chief Counsel, the ICE Office of the Chief Counsel, or the U.S. Attorney's Office, including a specific requirement that the officer or agent do so whenever a lawyer asserts that an electronic device contains privileged or confidential client information and the officer or agent continues to seek access to that information.

Thank you for your consideration of these issues. I look forward to your reply and working with you to ensure that the public has appropriate confidence that our homeland security institutions, agents, and officers respect the critical role that privileged and confidential communications between lawyers and their clients play in our free society.

Sincerely,

Linda Klein

Linda Klein
President, American Bar Association

cc: The Honorable Jeff Sessions, Attorney General, United States Department of Justice
Kevin K. McAleenan, Acting Commissioner, United States Customs and Border Protection
Scott K. Falk, Chief Counsel, United States Customs and Border Protection
Thomas D. Homan, Acting Director, United States Immigration and Customs Enforcement
Tracy Short, Principal Legal Advisor, United States Immigration and Customs Enforcement