Electronic Device Advisory for Mid-Year Meeting Attendees[1]

Thousands of lawyers, judges and other legal professionals will cross international borders when attending the 2018 ABA Mid-Year Meeting in Vancouver, British Columbia, Canada. Each person leaving and reentering the United States is subject to inspection and search from both United States and Canadian officials.

This paper has been prepared by the ABA Center for Professional Responsibility to update legal professionals about searches that U.S. Customs and Border Protection ("CBP") agents might conduct when legal professionals cross an international border with electronic devices containing confidential client or judicial information. While the actual number of travelers whose electronic devices are subject to border inspection is relatively low, a possibility exists that electronic devices may be searched.

Part I describes a new Directive, issued January 4, 2018, by the CBP. Part II summarizes the principal Model Rules of Professional Conduct legal professionals should consider. Part III offers a list of protective measures legal professionals may wish to take while planning their travel to the Mid-Year Meeting.

I. The Directive

On January 4, 2018, CBP issued a new Directive for border searches of electronic devices. This Directive, superseding one issued in 2009, applies to "[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and media players." These devices are hereinafter referred to collectively as "electronic devices."

---

[1] This paper has been prepared by Hon. Daniel J. Crothers, Justice of the Supreme Court of North Dakota and member of the ABA Standing Committee on Ethics and Professional Responsibility ("SCEPR") and Barbara S. Gillers, Adjunct Professor of Law at New York University School of Law and Chair of SCEPR, and is intended to provide legal professionals with general information about issues that could arise when engaged in international travel. Nothing in this paper is intended as providing legal advice, or creating a lawyer-client relationship between any party or entity involved. Legal professionals are encouraged to fully read other resources on this topic, and non-lawyers are encouraged to seek legal advice before taking any action in the area(s) covered by this paper. Further, this paper addresses only the activities of U.S. Customs and Border Protection (CBP) agents. Travelers should consult appropriate other sources for information on inspections and searches Canadian agents may conduct and how to respond. For example, the Canadian Border Security Agency (CBSA) has a written internal policy (CBSA Operational Bulletin PRG 2015-31 "Examination of Digital Devices and Media at Port of Entry") that is not published on the CBSA web-site, but may be available through the CBSA Access to Information process. The following third-party link may provide access to CBSA Operational Bulletin PRG 2015-31. http://www.lexsage.com/documents/CBSA%20Operational%20Bulletin%20PRG-2015-31%20Examination%20of%20Digital%20Devices%20and%20Media%20at%20Port%20of%20Entry.pdf.

The Directive contains CBP's claim of authority to conduct suspicionless border searches of all inbound and outbound travelers and their personal property—including electronic devices. The Directive further states:

> CBP' s broad authority to conduct border searches is well-established, and courts have rejected a categorical exception to the border search doctrine for electronic devices. Nevertheless, as a policy matter, this Directive imposes certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure that the authority for border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust.

Importantly, CBP notes "This Directive does not limit CBP's authority to conduct other lawful searches of electronic devices, such as those performed pursuant to a warrant, consent, or abandonment, or in response to exigent circumstances." While legal professionals likely cannot control whether a border search is conducted under authority of a warrant or in response to exigent circumstances, we can and arguably must control whether searches of electronic devices are conducted by consent, or after a lawful "demand" is made by CBP.[2]

The Directive describes the scope of permissible searches and states that "searches of electronic devices may include searches of the information stored on the device when it is presented for inspection or during its detention by CBP for an inbound or outbound border inspection." The Directive then describes how the scope of the searches it permits *is narrower* than the scope of searches permitted by the 2009 guidance. The Directive states "The border search will include an examination of *only the information that is resident upon the device* and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely." (Emphasis added.)

II. Principal Model Rules of Professional Conduct to Consider

Several Model Rules of Professional Conduct ("Rules") should be considered when deciding how to protect client confidential information on electronic devices during international travel.[3]

---

[2] The Directive is available at: https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/cbp-directive-3340-049a-border-search-electronic-media.pdf. It contains a description of procedures for handling electronic devices. It also states "This Directive is an internal policy statement of U.S. Customs and Border Protection and does not create or confer any rights, privileges, or benefits on any person or party." The Department of Homeland Security also recently released information about the number and nature of electronic device border searches. This document is available at https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.

[3] This paper is focused on a lawyer's ethical obligations to protect client information. For judges travelling internationally while carrying electronic devices containing confidential information, the applicable portions of the Model Code of Judicial Conduct are less apparent. Nevertheless, judges are advised to consider exercising the same precautions lawyers follow to avoid possibly violating Model Code of Judicial Conduct Rules 1.1 (Compliance with the Law), 1.2 (Promoting Confidence in the Judiciary, 2.2 (Impartiality and Fairness), 2.5 (Competence,

These include Rule 1.1 (on competence), Rule 1.6 (on client confidential information), Rules 5.1 and 5.3 (on supervisory duties), and Rule 1.4 (on communication). Other sources of protection for confidential information should also be considered, e.g. attorney-client privilege, the word product doctrine, and any statutory or common law protections that may apply in the legal professional's licensing jurisdiction.

Rule 1.1 requires that lawyers be competent in their representation of clients. Comment [8] to Rule 1.1 includes the admonition that "to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

Rules 5.1 and 5.3 impose supervisory obligations that travellers may wish to take into account. Rule 5.1 requires partners and "lawyer[s] who individually or together with other lawyers possesses comparable managerial authority in a law firm" to "make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules." Rule 5.1 requires certain supervisory lawyers to "make reasonable efforts to ensure that" the supervised lawyer "conforms to the Rules." Rule 5.3 imposes similar obligations toward employed, retained, or associated nonlawyers.

Rule 1.6(a) regulates disclosure and use of information relating to the representation of clients. This includes information that may be stored on a legal professional's electronic device.

Rule 1.6(a) provides "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b)."

Rule 1.6(c) requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to" information relating to the representation of a client. "Unauthorized access" refers to access that is not authorized *by the client*. See, e.g. Comments [5] and [15] to Rule 1.6 (indicating that "authorization" must be given by the client, not the lawyer). Comment [18] to Rule 1.6 allows that "The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure."[4]

Rule 1.4 contains a general duty to keep clients informed about their matters. If information relating to the representation of a client is disclosed during a border search, legal professionals

---

Diligence, and Cooperation), 2.9 (Ex Parte Communications), 2.10 (Judicial Statements on Pending and Impending Cases), 3.1 (Extrajudicial Activities) and 3.5 (Use of Nonpublic Information).

[4] See also, ABA Formal Op. 11-459 (Aug. 4, 2011) (an attorney's duty to "act competently to protect the confidentiality of clients' information . . . is implicit in the obligation of Rule 1.1 to 'provide competent representation to a client'").

should consider whether the rules of the professional's licensing jurisdiction require disclosure to the affected clients.[5]

Applying these Rules, a legal professional should consider whether consenting to a "request" by a CBP officer to search an electronic device containing client information would violate an ethical obligation.

On the other hand, if a CBP officer makes a "demand" under authority of the Directive or otherwise, a legal professional should consider whether disclosure is permitted under Model Rule 1.6(b)(6), which provides "A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary . . . to comply with other law or a court order." New York City Bar Association ("NYCBA") Formal Ethics Opinion 2017-5 speaks directly to this issue and concludes "Rule 1.6(b)(6) permits an attorney to comply with a border agent's demand, under claim of lawful authority, for an electronic device containing confidential information during a border search." However, the NYCBA Opinion continues, "compliance is not 'reasonably necessary' unless and until an attorney undertakes reasonable efforts to dissuade border agents from reviewing clients' confidential information or to persuade them to limit the extent of their review."

NYCBA Opinion 2017-5 preceded the release of the new CBP Directive by more than 6 months. But it is consistent with both Comment [18] to Model Rule 1.6 (suggesting that the lawyer take reasonable measures to prevent unauthorized access to client confidential information), and the protocols for CBP agents that are contained in the new Directive. Those protocols provide:

> Border searches may be performed by an Officer or other individual authorized to perform or assist in such searches (e.g., under 19 U.S.C. § 507).
>
> Border searches of electronic devices may include searches of the information stored on the device when it is presented for inspection or during its detention by CBP for an inbound or outbound border inspection. The border search will include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any

[5] See, e.g. New York City Bar Association (NYCBA) Opinion 2017-5, which concludes "if [an] attorney discloses clients' confidential information to a third party during a border search, the attorney must inform affected clients about such disclosures." NYCBA Opinion 2017-5 is discussed *infra* at p. 4 and is available here: http://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/formal-opinion-2017-5-an-attorneys-ethical-duties-regarding-us-border-searches-of-electronic-devices-containing-clients-confidential-information.

> network (e.g., by placing the device in airplane mode), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers should also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.

Legal professionals should advise the CBP officer that a device contains confidential information because the new Directive describes procedures that are to be followed once the CBP officer is so notified:

> Officers encountering information they identify as, or that is asserted to be, protected by the attorney-client privilege or attorney work product doctrine shall adhere to the following procedures.
>
> The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.
>
> Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/ Assistant Chief Counsel office. In coordination with the CBP Associate/ Assistant Chief Counsel office, which will coordinate with the U.S. Attorney's Office as needed, Officers will ensure the segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also ensuring that CBP accomplishes its critical border security mission. This segregation process will occur through the establishment and employment of a Filter Team composed of legal and operational representatives, or through another appropriate measure with written concurrence of the CBP Associate/ Assistant Chief Counsel office.

The new CBP Directive also addresses the handling of electronic devices that are encrypted or passcode protected. The Directive provides:

> Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode or encryption or other security mechanism, an Officer may request the individual's assistance in presenting the electronic device and the information contained therein in a condition that allows inspection of the device and its contents. Passcodes or other means of access may be requested and retained as needed to facilitate the examination of an electronic device or information contained on an electronic device, including information on the device that is accessible through software applications present on

the device that is being inspected or has been detained, seized, or retained in accordance with this Directive.

Passcodes and other means of access obtained during the course of a border inspection will only be utilized to facilitate the inspection of devices and information subject to border search, will be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be utilized to access information that is only stored remotely.

If an Officer is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the Officer may, in accordance with section 5.4 below, detain the device pending a determination as to its admissibility, exclusion, or other disposition.[6]

III. Measures Legal Professional Should Consider

In view of the foregoing, the following measures should be considered by all legal professionals travelling to Canada for the Mid-Year Meeting:

- Determine whether any electronic device that is necessary for your international travel contains information relating to the representation of a client, information protected by the attorney-client privilege or as attorney work product, or judicial or adjudicative information and material that is confidential (collectively, "confidential information"). Eliminate or minimize the number of these electronic devices that are in your possession when travelling.

- If an electronic device is necessary during the trip, minimize the amount of confidential information contained on the device. Remember that with electronically stored information, "delete" almost never fully removes all data.

- Consider obtaining a new but inexpensive electronic device. Place only necessary information on the device, and minimize or avoid placing confidential information on the device. Consider whether confidential information on the device should be encrypted. But keep in mind that CPB may demand that you unencrypt or unlock information, and, if you are unable to do so, CPB may detain the device.

- Have a working knowledge of the type and location of confidential information on any electronic device you do carry.

[6] Beyond the scope of this paper is the nature and depth of suspicionless searches CBP claims it can perform on an electronic device seized during a border search, what CBP claims it can do with recovered data, and how long that data can and will be retained. For more information, consult the Directive.

- Before approaching a border inspection area, consider placing electronic devices in "airplane" mode or having all wi-fi, Bluetooth and cellular connections terminated and disabled. Consider whether electronic devices should be powered down or locked.

- If subject to border inspection of electronic devices, determine whether the officer is making a "request" or a "demand" for inspection. Consider whether the Rules of Professional Conduct in your jurisdiction of licensure would permit you to consent to a "request" for inspection, or to accede to a "demand."

- If subject to border inspection of electronic devices, be prepared to identify yourself as a lawyer, judge or other legal professional and advise the officer that the electronic devices contain confidential information. Consider having available your bar admission card, business card, judicial identification(s) or other evidence that you are a legal professional.

- If subject to border inspection of electronic devices, consider the extent to which the Rules of Professional Conduct in your jurisdiction(s) of licensure require you to safeguard confidential information against unauthorized access by third parties and against inadvertent or unauthorized disclosure.

- If subject to border inspection of electronic devices, consider whether the Rules of Professional Conduct in your jurisdiction(s) of licensure require you to notify all clients whose information was or may have been revealed during the border search

Dated: January 10, 2018