Electronic Device Advisory for Mid-Year Meeting Attendees

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%202015-31%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

---


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 work 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.”

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

---

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 CPB claims it can perform on an electronic device seized during a border search, what CPB 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
COMMITTEE REPORT

Formal Opinion 2017-5: An Attorney’s Ethical Duties Regarding U.S. Border Searches of Electronic Devices Containing Clients’ Confidential Information*

May 09, 2018

VIEW REPORT

TOPIC: Duty to protect clients’ confidential information from disclosure that the client has not authorized; disclosure when border agents claiming lawful authority request access to clients’ confidential information; obligations upon disclosing clients’ confidential information.

DIGEST: Under the New York Rules of Professional Conduct (the “Rules”), a New York lawyer has certain ethical obligations when crossing the U.S. border with confidential client information. Before crossing the border, the Rules require a lawyer to take reasonable steps to avoid disclosing confidential information in the event a border agent seeks to search the attorney’s electronic device. The “reasonableness” standard does not imply that particular protective measures must invariably be adopted in all circumstances to safeguard clients’ confidential information; however, this opinion identifies measures that may satisfy the obligation to safeguard clients’ confidences in this situation. Additionally, Under Rule 1.6(b)(6), the lawyer may not disclose a client’s confidential information in response to a claim of lawful authority unless doing so is “reasonably necessary” to comply with a border agent’s claim of lawful authority. This includes first making reasonable efforts to assert the attorney-client privilege and to otherwise avert or limit the disclosure of confidential information. Finally, if the attorney discloses clients’ confidential information to a third party during a border search, the attorney must inform affected clients about such disclosures pursuant to Rule 1.4.

RULES: 1.1, 1.4, 1.6

QUESTION: What are an attorney’s ethical obligations with regard to the protection of confidential information prior to crossing a U.S. border, during border searches and thereafter?

OPINION:

I. Introduction
This opinion considers attorneys' ethical obligations in the context of the following scenario:

An attorney traveling abroad with an electronic device (such as a smartphone, portable hard drive, USB “thumb drive,” or laptop) that contains clients' confidential information plans to travel through a U.S. customs checkpoint or border crossing. During the crossing, a U.S. Customs and Border Protection (“CBP”) agent claiming lawful authority demands that the attorney “unlock” the device and hand it to the agent so that it may be searched. The attorney has not obtained informed consent from each client whose information may be disclosed in this situation.[1]

Searches of electronic devices at the U.S. border when travelers enter or leave the U.S. may include not only a physical inspection of these devices but also the review of information stored on them, such as emails, text messages, and electronically-stored documents.[2] CBP policy permits U.S. customs agents to review any information that physically resides on travelers' electronic devices, including those of U.S. citizens, with or without any reason for suspicion, to demand disclosure of social media and email account passwords, and to seize the devices pending an inspection.[3] In recent years, searches of cell phones, laptop computers, and other electronic devices at border crossings into the U.S. have become increasingly frequent. According to the Department of Homeland Security, more than 5,000 devices were searched by CBP agents in February 2017 alone. By way of comparison, that is about as many U.S. border searches of electronic devices as were undertaken in all of 2015, and just under a quarter of the approximately 23,877 U.S. border searches of such devices undertaken in 2016. Further, border agents have access to software tools that increase the effectiveness and thoroughness of device searches, and they have the ability to copy the contents of such devices to be reviewed later. To be sure, the 5000-plus individuals whose devices were searched in February 2017 amounted to only a fraction of the 1,069,266 individuals entering into the United States daily as reported by the CBP.[4] However, depending on the extent of the search, border agents’ review of information stored on, or accessible via, individuals’ electronic devices may lead to the disclosure of substantial information, and therefore constitute a significant intrusion for the selected individuals.[5] Under these circumstances, attorneys would benefit from guidance regarding their ethical obligations prior to crossing a U.S. border and when confronted with a border agent’s request to search electronic devices containing clients’ confidential information.[6]

This Opinion addresses an attorney's ethical obligations under the Rules with respect to U.S. border searches of electronic devices containing clients’ confidential information at three points in time: before the attorney approaches the U.S. border; at the border when U.S. border agents seek to review information on the attorney's electronic device; and after U.S. border agents review clients’ confidential information.
Before crossing the U.S. border, both Rule 1.6(c), which requires “reasonable efforts to prevent . . . unauthorized access to” clients' confidential information, and the duty of competence under Rule 1.1, require an attorney to take reasonable measures in advance to avoid disclosing confidential information in the event border agents seek to search the attorney's electronic device. The “reasonableness” standard does not imply that particular protective measures must invariably be adopted in all circumstances to safeguard clients' confidential information; however, this Opinion identifies measures that may satisfy the obligation to safeguard clients' confidences in this situation.

At the border, if government agents seek to search the attorney's electronic device pursuant to a claim of lawful authority,[7] and the device contains clients' confidential information, the attorney may not comply unless “reasonably necessary” under Rule 1.6(b)(6), which permits disclosure of clients' confidential information to comply with “law or court order.” Under the Rule, the attorney first must take reasonable measures to prevent disclosure of confidential information, which would include informing the border agent that the device or files in question contain privileged or confidential materials, requesting that such materials not be searched or copied, asking to speak to a superior officer and making any other lawful requests to protect the confidential information from disclosure. To demonstrate that the device contains attorney-client materials, the attorney should carry proof of bar membership, such as an attorney ID card, when crossing a U.S. border.

Finally, if the attorney discloses clients' confidential information to a third party during a border search, the attorney must inform affected clients about such disclosures pursuant to Rule 1.4.

II. Before Crossing the U.S. Border Attorneys Must Undertake Reasonable Efforts to Protect Confidential Information

Attorneys have a duty under Rule 1.6 to protect clients' confidential information.[8] Rule 1.6(a) provides that an attorney may not knowingly use or disclose confidential information without the client's informed consent or implied authorization. Few principles are more important to our legal system.

Additionally, an attorney's obligation to safeguard clients' confidential information against unintentional or unauthorized disclosure is implicit in the duty of competence under Rule 1.1. See 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'”); cf. NYCBA Formal Op. 2015-3 (April 2015) (“In our view, the duty of competence includes a duty to exercise reasonable diligence in identifying and avoiding common Internet-based scams, particularly where those scams can harm other existing clients.”).
Further, the obligation to safeguard clients' confidences is now codified in Rule 1.6(c), as amended January 1, 2017, which specifically requires attorneys to "make reasonable efforts to prevent the inadvertent or unauthorized use or disclosure of, or unauthorized access to," confidential information obtained from prospective, current, and former clients. See Rule 1.1, cmts.[16] & [17]. The duty to protect client confidences from "unauthorized access" refers to access that is not authorized by the client. Cf. Rule 1.6, cmts. [5] & [13] (indicating that "authorization" must be given by the client, not the lawyer). Consequently, just as lawyers must take reasonable measures to prevent third parties' unlawful access to client confidences, attorneys must refrain from conduct, including otherwise permissible disclosures, that may result in third parties' lawful access to a client's confidential information without the client's consent. See, e.g., NYCBA Formal Op.2017-2 (Feb. 2017) (an attorney may not report attorney misconduct to the disciplinary authority where doing so might lead the disciplinary authority to require the production of a client's confidential information without the client's consent).

Prior opinions have recognized, in particular, that the duty to safeguard clients' confidences includes a responsibility to take reasonable protective measures when engaging in electronic communications with clients and in electronically storing clients' confidential information. See, e.g., ABA Formal Op. 477R (May 11, 2017); ABA Formal Op. 11-459 (Aug. 4, 2011); ABA Formal Op. 99-413 (March 10, 1999); Cal. Ethics Op. 2010-179 (Jan. 1, 2010); NYSBA Ethics Op. 842 (Sept. 10, 2010); NYSBA Ethics Op. 709 (Sept. 16, 1998). To be "reasonable," protective measures need not be foolproof: making reasonable efforts "does not mean that the lawyer guarantees that the information is secure from any unauthorized access." NYSBA Ethics Op. 842, supra. Further, the adequacy of an attorney's efforts to protect clients' confidences depends upon a multitude of facts. See, e.g., ABA Formal Op. 477R, supra ("Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule1.6(c) includes nonexclusive factors to guide lawyers in making a 'reasonable efforts' determination."); ABA Formal Op. 11-459, supra ("particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters").

Rules 1.1 and 1.6(c) require attorneys to make reasonable efforts prior to crossing the U.S. border to avoid or minimize the risk that government agents will review or seize client confidences that are carried on, or accessible on, electronic devices that attorneys carry across the border. Except in the unlikely event that an attorney has each affected client's consent to disclose confidential information during a border search, such disclosure would be "unauthorized" under Rule 1.6(c) and the attorney would be obligated to make "reasonable efforts" to prevent such disclosure from occurring. In the above hypothetical, the attorney has not obtained informed consent from the clients whose confidential information would be affected, as is required to obtain authorization under Rule 1.6(a)(1). Further, it is hard to imagine a situation where disclosure to a government official during a border search would "advance the
best interests of the client” and therefore be “implicitly authorized to advance the best interests of the client” under Rule 1.6(a)(2).

The necessary degree of precaution depends on the circumstances, including the sensitivity of the confidential information that is at risk. See Rule 1.6, cmt. [16] (listing relevant considerations). “Reasonableness” by its nature depends on the multiple facts and circumstances of a given situation and does not lend itself to categorical or bright-line rules. If in doubt, an attorney may, and would be well-advised to, take more cautious measures than what is minimally required by Rule 1.6(c).

Comment[16] to Rule 1.6 provides guidance by identifying the following non-exclusive list of factors relevant to the reasonableness of an attorney’s efforts:

1. The sensitivity of the information;
2. The likelihood of disclosure if additional safeguards are not employed;
3. The cost of employing additional safeguards;
4. The difficulty of implementing the safeguards; and
5. The extent to which the safeguards adversely affect the attorney’s ability to represent clients (e.g., by making a device or software excessively difficult to use).

Thus, the various facts and circumstances bearing on whether protective efforts are “reasonable” to avoid disclosing client confidences at the border – and therefore minimally required by Rule 1.6(c) – may include the type and nature of the confidential information involved; the need to bring the information across the border in the first instance; the safeguards used by the attorney; the availability, costs, and challenges associated with implementing additional safeguards; an attorney’s resources and capabilities; and any factors that may affect the likelihood of disclosure, such as the jurisdiction from which the attorney is returning. Among other things, these considerations suggest that an attorney should not carry clients’ confidential information on an electronic device across the border except where there is a professional need to do so, and especially that attorneys should not carry clients’ highly sensitive information except where the professional need is compelling. [9]

Given the rapid pace of technological development and the disparities between the practices, capabilities, and resources of attorneys, it would be difficult or impossible to identify a list of minimum mandatory prophylactic or technical measures for an attorney to adopt before crossing the U.S. border. Not only would such a list run the risk of quickly becoming obsolete, but it would also be of limited use, since “reasonableness” standards are not amenable to a one-size-fits-all analysis. Moreover, expectations regarding reasonable efforts are likely to evolve over time as the relevant technology changes, as practices regarding border searches and knowledge of those practices develop, and as attorneys become increasingly aware of the risks of disclosure and the available means to avoid them. However, as discussed
below, an attorney must generally (i) evaluate the risks presented by traveling with confidential information and (ii) based on the risk analysis, consider what safeguards to employ to limit or reduce the risk that confidential information will be accessed or disclosed in the event of a search. While no particular safeguard is invariably required by the Rules as long as the attorney’s protective efforts are “reasonable,” we recommend that attorneys consider adopting the following safeguards to protect confidential information or to reduce the risk of its disclosure.

i. Evaluating the Risk of Disclosure and Potential Harms that May Result

An attorney must evaluate the risks associated with crossing the U.S. border while in possession of clients’ confidential information, including the likelihood that border agents will demand and secure disclosure of clients’ confidential information, the sensitivity of the information carried, and the harm that would result if the information were disclosed. This requires familiarity with the relevant laws and practices regarding border searches of electronic devices whenever an attorney opts to carry a device that contains, or can access, clients’ confidential information. Cf. NYSBA Ethics Op. 782 (Dec. 8, 2004) (requiring lawyers to use “reasonable care” to stay abreast of technological advances and the potential risks associated with using, storing, maintaining, accessing, and transmitting confidential information).

Although, as noted above, U.S. border searches of electronic devices (at the time of this opinion’s publication) are relatively infrequent, any unauthorized disclosure of a client’s confidential information entails a violation of the client’s expectation of confidentiality and is presumptively harmful, regardless of whether the unauthorized recipient otherwise uses the information to the client’s detriment. See, e.g., NYCBA Formal Op. 2017-2, supra (attorney may not provide client’s confidential information to the disciplinary authority without the client’s consent, even if the client would not be “embarrassed or harmed if the information were disclosed to the disciplinary authority specifically”). Moreover, even if a border search seems highly unlikely, that consideration should be weighed against the amount and sensitivity of the information held and any additional harm that may result from its disclosure without the client’s consent.[10] For certain lawyers, practices, organizations, or clients, providing government agencies with access to sensitive confidential data can cause significant harm, which would strongly suggest in such circumstances that it would be unreasonable to carry confidential information that may be disclosed to border agents, even for legitimate professional reasons, if avoidable.

ii. Implementing Safeguards

Attorneys must also evaluate the efficacy, cost, and difficulty associated with implementing safeguards to prevent or limit confidential information. Rule 1.6, cmt. [16].[11] As discussed above, whether safeguards are ultimately required as minimally “reasonable efforts” depends on the circumstances of each such situation.
The simplest option with the lowest risk is not to carry any confidential information across the border. One method of avoiding the electronic transportation of clients' confidences involves using a blank "burner" phone or laptop, or otherwise removing confidential information from one's carried device by deleting confidential files using software designed to securely delete information, turning off syncing of cloud services, signing out of web-based services, and/or uninstalling applications that provide local or remote access to confidential information prior crossing to the border.[12] This is not to say that attorneys traveling with electronic devices must remove all electronically stored information. Some electronic information, including many work-related emails, may contain no confidential information protected by Rule 1.6(a). Even when emails contain confidential information, the obligation to remove these emails from the portable device before crossing the border depends on what is reasonable. As previously discussed, this turns on the ease or inconvenience of avoiding possession of confidential information; the need to maintain access to the particular information and its sensitivity; the risk of a border inspection; and any other relevant considerations.

A lawyer with access to greater resources or who handles more sensitive information should consider technological solutions that permit secure remote access to confidential information without creating local copies on the device; storing confidential information and communications in secure online locations rather than locally on the device; or using encrypted software to attempt to restrict access to mobile devices.

While attorneys thus have various available alternative means of safeguarding clients' confidential information from disclosure at the U.S. border, whatever measures an attorney adopts must, under all the facts and circumstances, be "reasonable" to protect this information.[13]

III. At the U.S. Border Attorneys May Disclose Clients' Confidential Information Only to the Extent "Reasonably Necessary" to Respond to a Government Agent's Claim of Lawful Authority

Assuming an attorney has made reasonable efforts to protect clients' confidential information before crossing the U.S. border, in many cases the attorney will entirely avoid carrying clients' confidential information in an electronic device. In other cases, when attorneys' electronic devices do contain clients' confidential information, the information will be limited to what is professionally necessary, and ideally limited insignificance, so that clients would not be significantly harmed by its disclosure. But regardless of how limited or insignificant the information may appear to be, attorneys subject to a border search may disclose clients' confidential information only to the extent permitted by Rule 1.6.

Rule 1.6(a) prohibits attorneys from knowingly disclosing "confidential information" or using such information to the disadvantage of the client, for the lawyer's own
advantage, or for the advantage of a third person, unless the client gives informed consent or implied authorization or the disclosure is permitted by Rule 1.6(b). Rule 1.6(b), in turn, permits, but does not require, an attorney to use or disclose confidential information in specified exceptional circumstances, of which only 1.6(b)(6) is relevant to the above-described border-search scenario.

Rule 1.6(b)(6) permits an attorney to “reveal or use” confidential information to the extent the attorney “reasonably believes necessary . . . when permitted or required . . . to comply with other law or court order.” Comment [13] to Rule 1.6 recognizes that this exception permits the disclosure of a client’s confidential information insofar as reasonably necessary to respond to an order by a “governmental entity claiming authority pursuant to . . . law to compel disclosure.” The exception applies even when the validity of the relevant law or court order, or its application, is subject to legal challenge, although, in ordinary circumstances, compliance is not “reasonably necessary” until any available legal challenge has proven unsuccessful. See Rule 1.6, cmt. [13] (“Absent informed consent of the client to comply with the order, the lawyer should assert on behalf of the client non-frivolous arguments that the order is not authorized by law, the information sought is protected against disclosure by an applicable privilege or other law, or the order is invalid or defective for some other reason.”).

In general, disclosure of clients’ confidential information is not “reasonably necessary” to comply with law or a court order if there are reasonable, lawful alternatives to disclosure. Even when disclosure is reasonably necessary, the attorney must take reasonably available measures to limit the extent of disclosure. See, e.g., ABA Formal Op. 10-456 (July 14, 2010). For example, compliance with asubpoena or court order to disclose confidential information is not “reasonably necessary” until the attorney or the attorney’s client (or former client) has asserted any available non-frivolous claim of attorney-client privilege. See, e.g., NYCBA Formal Op. 2005-3 (March 2005). Likewise, a lawyer must ordinarily test a government agency’s request for client confidential information made under color of law. See, e.g., NYCBA Formal Op. 1986-5 (July 1986) (“If presented with a request by a governmental authority for production of information pertaining to escrow accounts when a client is a target of an investigation, a lawyer must, unless the client has consented to disclosure, decline to furnish such information on the ground either that it is protected by the attorney-client privilege or that it has been gained in the course of a confidential relationship. . . . If disclosure is [subsequently] compelled [by a court], it will not breach a lawyer’s ethical obligation with respect to his client’s confidences or secrets.”).

At the same time, attorneys need not assume unreasonable burdens or suffer significant harms in seeking to test a law or court order. See, e.g., NYSBA Ethics Op. 945 (Nov. 7, 2012) (indicating that “when the law governing potential disclosure is unclear, a lawyer need not risk violating a legal or ethical obligation, but may disclose client confidences to the extent the lawyer reasonably believes it is necessary to do so.
to comply with the relevant law, even if the legal obligation is not free from doubt").
For example, although an attorney must consult with the client about an adverse
ruling, see Rule 1.4, the attorney need not finance an appeal of the court's ruling much
less intentionally defy the trial courtand accept a contempt-of-court order. See, e.g.,
ABA Formal Op. 473 (Feb. 17, 2016) ("Requiring a lawyer to take an appeal when the
client is unavailable places significant and undue burdens on the lawyer."); NYCBA
Formal Op. 2005-3, supra ("Should the court overrule the objection or assertion of
privilege or other protection, the attorney may then testify about the privileged or
protected material").

Rule 1.6(b)(6) permits an attorney to comply with a border agent's demand, under a
claim of lawful authority, for an electronic device containing confidential information
during a border search. While legal challenges in court might be made to the relevant
law or its application, it would be an unreasonable burden to require that attorneys,
having made reasonable efforts to protect clients' confidential information, forgo
reentry into the United States or allow themselves to be taken into custody while
litigating the lawfulness of a border search. Unless court rulings forbid such border
searches, an attorney may ultimately comply with a border agent's demand. Likewise,
in this unusual circumstance, it would ordinarily be impracticable and of no utility for
attorneys stopped at the border to consult with the affected clients before
complying. (The obligation to consult thereafter is addressed below in Part IV.)

That said, 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.
Accord Rule 1.6(c) (requiring “reasonable efforts” to protect clients' confidential
information). Such efforts would include informing the border agent that the subject
devices or files contain privileged or confidential materials, requesting that such
materials not be searched or copied, asking to speak to a superior officer and making
any other reasonably available efforts to protect the confidential information from
disclosure. To add credence to the claim of attorney-client privilege, an attorney
should carry and be prepared to present some form of attorney identification, such
as a court-issued identification or in the very least a business card, when crossing a
U.S. border. An attorney should know the relevant law and practices and should
consider bringing a printed copy of a given customs agency’s policies or guidelines
regarding searches of privileged information. [14]

The practical significance of clearly informing the border agent of the presence of
confidential or privileged information arises from the regulations of the CBP and the
U.S. Immigration and Customs Enforcement Bureau ("ICE"), which each recognize the
sensitivity of legal materials. The regulations require a border agent confronted with
a claim of legal privilege to seek an additional review or authorization prior to
conducting a search of the information that the attorney claims is confidential or
privileged. This obligation to obtain further review applies "only to the extent that the
agent 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 or ICE, respectively.[15] Although it is uncertain how border agents apply this “suspicion” standard in actual searches, attorneys should take advantage of this possible avenue for preventing the disclosure of clients' confidential information.

IV. If Confidential Information Is Disclosed During a Border Search, An Attorney Must Promptly Inform Affected Clients

If an attorney's electronic device containing clients' confidential information is reviewed or seized at the border, the attorney must notify affected clients of what occurred and of the extent to which their confidential information may have been reviewed or seized.[16] This obligation arises out of the general duty under Rule 1.4 to communicate with the client about the status of a matter and about decisions that the client faces in the representation. See Rule 1.4(a)(1)(i) & (a)(3); see also Rule 1.6, cmt. [13]; compare NYCBA Formal Op. 2015-6 (June 2015) ("Given that lawyers have a duty to preserve client files (at least for some period of time), it follows that an attorney may have a duty to notify the client or former client when such files have been inadvertently destroyed."); NYSBA Ethics Op. 1092 (May 11, 2016) ("a lawyer must report to a client a significant error or omission by the lawyer in his or her rendition of legal services"). Disclosure will provide the client an opportunity to determine whether to file a legal challenge, assuming one is available, or to undertake any other available responses. Whether attorneys have legal obligations in this situation independently of the Rules is a question outside the scope of this opinion.

CONCLUSION:

Before crossing the U.S. border, an attorney must make reasonable efforts to protect against the disclosure of clients' confidential information in response to a demand by border agents. Because “reasonable efforts” depend on the circumstances, no particular safeguards are invariably required. However, attorneys should generally (i) evaluate the risks of traveling with confidential information and (ii) consider what safeguards to implement to avoid or reduce the risk that confidential information will be accessed or disclosed in the event of a search. At the border, if government agents seek to search the attorney's electronic device pursuant to a claim of lawful authority, and the device contains clients' confidential information, the attorney may not comply until first making reasonable efforts to assert the attorney-client privilege and to otherwise avert or limit the disclosure of confidential information, e.g., by asking to speak to a superior officer. To add credence to the claim of attorney-client privilege, an attorney should carry attorney identification and be familiar with the customs agency's policies or guidelines regarding searches of privileged information. Finally, if the attorney discloses clients' confidential information to a third party during a border search, the attorney must inform affected clients about such disclosures.
* After the opinion was issued in July 2017, U.S. Customs and Border Protection issued a revised Directive on Border Search of Electronic Devices (CBP Directive No. 3340-049A), dated January 2018, to “provide guidance and standard operating procedures” for border searches of electronic devices; and federal policy may continue to change. The general principles set forth in the opinion nonetheless remain applicable.

[1] This opinion does not address the potentially more difficult questions regarding an attorney’s duty to protect confidential information while in, or crossing into, foreign countries. While the principles described in this opinion regarding safeguarding clients’ confidential information are broadly applicable, efforts reasonably necessary to protect clients’ confidences at foreign borders and in foreign countries will vary depending on the laws and practices of those countries. Lawyers must therefore familiarize themselves with those laws and practices and determine what safeguards to adopt before transporting clients’ confidential information abroad.

[2] In this respect, border searches apparently differ from Transportation Security Administration (TSA) searches of electronic devices in connection with domestic air travel. This Opinion only addresses ethical issues in connection with international travel.

[3] See June 20, 2017 Due Diligence Questions for Kevin McAleenan, Nominee for Commissioner of U.S. Customs and Border Protection (CBP), available at: http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/170712-cpb-wyden-letter.pdf. According to this policy statement, CBP agents do not condition U.S. citizens’ reentry on the provision of passwords; nor do they currently review information that, although not physically resident on the devices, is accessible on remote servers via electronic devices. According to CPB, inspections may reveal that electronic devices contain contraband (e.g., child pornography), or that information on electronic devices reveals a threat to national security. CBP reserves the right to cooperate with other investigative agencies, which may seek other kinds of information on travelers’ electronic devices.

[4] U.S. Customs and Border Protection, Snapshot: a Summary of CBP Facts and Figures (2017), available at https://www.cbp.gov/sites/default/files/assets/documents/2017-Mar/CBP-Snapshot-UPDATE-03022017-FY16-Data.pdf (citing daily statistic of 1,069,266 average daily arrivals in February 2017; only 326,723 were by air). Based on these figures, only approximately 0.017% of all individuals entering the United States on a given day are subject to an electronic device search, even with the increase in such searches in 2017. There are no available statistics evidencing how many of the 5,000 searched devices belonged to members of the bar.


[6] These circumstances have prompted the ABA to seek changes and clarifications to existing regulations and practices regarding the treatment of confidential and privileged materials during border searches. See American Bar Association, Preservation of...


[8] Rule 1.6(a) defines "confidential information" as "information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential."

[9] An attorney whose client outside the United States provides electronically-stored confidential information (e.g., on a thumb drive) must "reasonably consult with the client about the means by which the client's objectives are to be accomplished." Rule 1.4(a)(2). The attorney should consider whether this obligation triggers, under all the circumstances, the need for a discussion concerning the manner in which the client's confidential information will be transported and the attendant risks.

[10] Traveling attorneys should also be aware that many customs and border protection agencies may demand that the attorney provide access to any information stored on a device (including information that may be otherwise protected or encrypted), and in addition may have access to software tools that allow them to copy the entirety of a device and/or permit the recovery of deleted information that has not been securely deleted using specialized tools. Test Results for Mobile Device Acquisition, DEPT. OF HOMELAND SECURITY, https://www.dhs.gov/publication/mobile-device-acquisition (last visited Apr. 11, 2017).

[11] Comment [16] further recognizes that a client may "require the lawyer to implement special security measures not required by this Rule, or ... give informed consent to forgo security measures that would otherwise be required by this Rule." As this Comment reflects, an attorney may not forgo "reasonable efforts" to protect the client's confidential information, as required by Rule 1.6(c), unless the client gives informed consent. Further, especially when it is necessary to travel with highly sensitive information, an attorney would be well advised to discuss with the client
whether to adopt special security measures, beyond those required by Rule 1.6(c) in the situation.

[12] Prior to any such deletion, however, an attorney should ensure that the information deleted is securely backed up so that the attorney may use the information at a later date.


[15] Section 5.2.1 of CBP Directive No.3340-49, provides: “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.” U.S. Customs and Border Protection Directive No. 3340-049, Border Search of Electronic Devices Containing Information (2009) available at https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf Section 8.6(2)(b) of the parallel ICE Directive similarly provides: “Special Agents may encounter information that appears to be legal in nature, or an individual may assert that certain information is protected by the attorney-client or attorney work product privilege. If Special Agents suspect that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of ICE, the ICE Office of the Chief Counsel or the appropriate U.S. Attorney’s Office must be contacted before beginning or continuing a search of the document and this consultation shall be noted in appropriate ICE systems.”

[16] In the context of responding to disclosures as a result of hacking, legal data security experts recommend, where possible, applying forensic analysis to systems after a breach occurs since the appropriate response must be guided by the scope of the breach. A similar approach may be warranted when an electronic device has been confiscated, i.e. a lawyer should take available steps to learn what was disclosed. See Allison Grande, 5 Steps to Take When Your Law Firm Is Hacked, Law360 (Jul 22, 2014) 16 PM EDT, https://www.law360.com/articles/556398/5-steps-to-take-when-your-firm-is-hacked
Reissued May 2018

Author(s): Professional Ethics Committee

Issue(s): Profession, Legal Education & Organization of the Bar

Subject Area(s): Ethics | Attorney/Client Confidentiality