fucile & reising | LLP

February 2026 WSBA *Bar News Ethics & the Law* Column

Crossing Over:
Confidentiality at International Borders

By Mark J. Fucile
Fucile & Reising LLP

Lawyers have been crossing international borders for a long time. John Adams, for example, sailed from Boston to France in 1778 to negotiate a treaty with the French during the Revolutionary War (only to learn that Benjamin Franklin had already done the deal).[1] What has changed over time, however, is the form and volume of client confidential material lawyers have with them when crossing international borders. Since the days of John Adams until fairly recently, paper was a lawyer's stock-in-trade. As such, a traveling lawyer might have a paper file or two when crossing a border related to the matters involving the business trip. By contrast, most law firm files today are electronic. Further, our electronic devices—whether laptops, tablets, or phones—often either carry or have access to all of our client files. Today's technology becomes a sensitive point at international borders because inspections of electronic devices do not necessarily include the same legal protections as when operating within a country. This puts a premium on carefully planning what we carry across international borders to protect client confidentiality.

In this column, we'll look at two aspects of lawyer confidentiality when crossing international borders.

First, we'll survey how our duty of confidentiality interfaces with the legal and regulatory mix governing electronic device inspections across borders. In doing so, we'll focus on return travel into the United States. That obviously leaves out the other 192 countries that are members of the United Nations.[2] Although the regulatory environment in those other countries varies, the general considerations we'll discuss apply with equal measure when entering another country. Further, part of a lawyer's trip preparation should include reviewing both the regulations governing entry inspections and how those regulations may be applied. Canada, the United Kingdom, and the European Union, for example, have readily available online descriptions of what travelers can expect.[3] Although admittedly a rough gauge, the State Department's travel advisory website is at least a starting point for assessing a particular country's likely adherence to its stated border inspection policies.[4]

Second, we'll then turn to practical precautions lawyers can take to protect client confidentiality. Although these steps involve technology, we'll aim not to be too technical. Further, although the focus is on the border, lawyers also need to

take reasonable steps to protect confidentiality when carrying and using electronic devices in a foreign country just as they would here.[5]

Confidentiality at the Border

Under RPC 1.6(c), "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[6] Comments 18 and 19 to RPC 1.6 underscore that our duty of confidentiality is also part of our duty of competent representation under RPC 1.1—with the title to those two comments neatly blending those duties: "Acting Competently to Preserve Confidentiality." Comments 18 and 19 explain that we need to take reasonable steps to protect confidential information when using electronic tools that are consistent with the sensitivity of the information involved.[7]

One of the leading bar opinions nationally on this topic—New York City Bar Formal Opinion 2017-5 (2017)—summarizes these twin duties[8] when carrying electronic devices with client information across a border:

> Rules 1.1 and 1.6(c) require attorneys to make reasonable efforts prior to crossing the . . . border to avoid or minimize the risk that government agents will review or seize 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 obliged to make "reasonable efforts" to prevent such disclosure from occurring. . . .
>
> The necessary degree of precaution depends on the circumstances, including the sensitivity of the confidential information that is at risk . . . "Reasonableness" by its nature depends on the multiple facts and circumstances of a given situation and does not lend itself to categorical bright-line rules."[9]

In addition to understanding the law practice technology that a lawyer is using, lawyers crossing the border with client confidential information also need to appreciate the basics of search and seizure law and Government inspection policies—neither of which is static.

On the former, although searches of cell phones and similar electronic devices within the country generally require a warrant,[10] decisional law currently suggests that cell phones and laptop computers are not immune from at least manual inspection under the "border exception" that allows searches without reasonable suspicion when entering the United States.[11] Pending definitive guidance from the United States Supreme Court, considerable nuance remains among the federal circuits that have spoken to the issue on the degree of suspicion (if any) required under the border exception for searches of electronic devices—especially those involving forensic examinations of the contents.[12]

On the latter, U.S. Customs and Border Protection has published its current guidance on its website.[13] CBP distinguishes between "basic" and "advanced" searches.[14] As updated earlier this year, CBP describes a "basic" search as an inspection that is primarily (*but not exclusively*) manual "in which an officer conducts a review or analysis of information residing in electronic or digital form on the device."[15] CBP defines an "advanced" search as involving the use of external equipment to review and analyze the contents of a device.[16] Under current CBP policy, an "advanced" search ordinarily requires reasonable suspicion of illegal activity.[17] Even with a "basic" search, however, CBP may "request" that a device be opened if password protected—with possible "detention" of the device if the traveler does not cooperate.[18] Although CBP policy includes a mechanism for segregating material otherwise protected by the attorney-client privilege or the work product rule,[19] it is important to remember that policies can change or simply be ignored.[20] Assessing both current CBP policy and how its stated policy is being applied in actual practice should ordinarily be part of a careful lawyer's "reasonable efforts" to protect client confidentiality under RPC 1.6(c).[21]

In light of this legal and regulatory uncertainty, the practical solutions discussed next, while not foolproof, offer a degree of personal control that simple reliance on the vagaries of the legal and regulatory environment does not.

Practical Precautions

Sources of practical guidance in this area are many and varied. Some address privacy concerns generally.[22] Others are tailored specifically to lawyers.[23] Although the available guidance varies in its technological granularity, three simple themes predominate.

First, when planning a trip, just bring what you need. Clearly, in an age of electronic airplane boarding passes, a phone is a practical necessity. If it is a vacation trip, however, a laptop computer stuffed with your work files may not be.

Second, remove confidential files from the devices you bring with you and access them remotely during the trip.[24] In some instances, a tablet may be a more convenient way to access necessary files remotely without deleting files from a work laptop before travel. In others, lawyers may consider using a separate "travel only" laptop that has the electronic features necessary for work (including remote access) but doesn't have the lawyer's files stored on the device itself.

Third, before crossing the border, sign-out of email apps, disconnect from remote access file storage, and turn off Wi-Fi and cell connections (or switch to "airplane mode") so that emails and remotely stored files will not appear on the device if inspected manually at the border. Under current CBP policy, inspectors are not supposed to use the device to access files stored remotely.[25]

If, nonetheless, you have inadvertently left a sensitive client document on your electronic device, politely let the CBP officer know you are a lawyer (and be prepared to present confirming identification[26]), let the officer know that you have documents covered by the attorney-client privilege or the work product rule on the device in an effort to dissuade the officer from reviewing them, and, if necessary, ask to speak to the officer's supervisor so that the confidential information can be segregated from the review.[27] Simply imagining this scenario at the end of a long trip may be enough to encourage most lawyers to leave confidential files behind.

ABOUT THE AUTHOR

Mark J. Fucile of Fucile & Reising LLP advises lawyers, law firms, and corporate and governmental legal departments throughout the Northwest on professional ethics and risk management. Mark has chaired both the WSBA Committee on Professional Ethics and its predecessor, the WSBA Rules of Professional Conduct Committee. Mark has served on the Oregon State Bar Legal Ethics Committee and is a member of the Idaho State Bar Section on Professionalism & Ethics. Mark writes the Ethics Focus column for the

Multnomah (Portland) Bar's *Multnomah Lawyer*, the Ethics & the Law column for the WSBA *Bar News* and is a regular contributor on legal ethics to the WSBA *NWSidebar* blog. Mark is the editor-in-chief and a contributing author for the WSBA *Legal Ethics Deskbook* and a principal editor and contributing author for the OSB *Ethical Oregon Lawyer* and the WSBA *Law of Lawyering in Washington*. Before co-founding Fucile & Reising LLP in 2005, Mark was a partner and in-house ethics counsel for a large Northwest regional firm. He also taught legal ethics for over a decade as an adjunct at the University of Oregon School of Law. Mark is admitted in Oregon, Washington, Idaho, Alaska and the District of Columbia. He is a graduate of the UCLA School of Law. Mark's telephone and email are 503.860.2163 and Mark@frllp.com.

---

[1] https://www.nps.gov/adam/john-adams-biography.htm?&NMW_TRANS=ext.

[2] https://www.un.org/en/about-us.

[3] *See, e.g.,* https://www.cbsa-asfc.gc.ca/travel-voyage/edd-ean-eng.html (Canada), https://www.gov.uk/uk-border-control (UK), https://european-union.europa.eu/live-work-study/travelling-eu_en (EU).

[4] *See* https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/.

[5] *See generally* ABA Formal Ops. 99-413 (1999) (email security), 477R (data transmission), 483 (cybersecurity); WSBA Advisory Op. 2215 (cloud computing); *see also* ABA, *Cybersecurity Handbook* (3d ed. 2022) (surveying a wide variety of cybersecurity risks to lawyers and law firms and how to protect against them).

[6] RPC 1.6 focuses on current clients. RPC 1.9(c), in turn, outlines the continuing duty of confidentiality to former clients.

[7] *See also* RPC 1.1, cmt. 8 (addressing the responsibility to stay current on the technology we use in law practice).

[8] The New York and Washington RPC are both drawn from their ABA Model Rule counterparts and largely mirror each other on the points discussed here.

[9] New York City Bar Formal Op. 2017-5 (2017) at 5. The New York City Bar opinion focuses on re-entry into the United States. Other comparatively recent bar resources on this topic include New Hampshire Bar Advisory Op. 2018-19/1 (2018), Candace M. Groth, "Crossing the Border: Tips for Attorneys," 78 No. 7 Bench & Bar of Minnesota 12 (Aug. 2019), and Wade v. Davis, "Taking Client Confidences on the Road," 57 Tenn. B.J. 46 (Mar./Apr. 2021). *See generally* ABA, *Annotated Model Rules of Professional Conduct* 155-56 (10th ed. 2023) (summarizing authorities nationally addressing confidentiality issues for portable electronic devices in the border search context).

[10] *See generally Riley v. California*, 573 U.S. 373, 134 S. Ct. 2473, 189 L. Ed.2d 430 (2014) (discussing cell phone searches).

[11] *See generally Unites States v. Ramsey*, 431 U.S. 606, 620, 97 S. Ct. 1972, 52 L. Ed.2d 617 (1977) (surveying border exception); *United States v. Cano*, 934 F.3d 1002 (9th Cir. 2019) (cell phone searches at the border and requiring reasonable suspicion for a "forensic" examination); *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (lap top computer searches at the border and requiring reasonable suspicion for "forensic" examination).

[12] For surveys of decisional law among the federal circuits—including the degree of suspicion required for detailed examinations of device content, *see* Philetus Holt, *Cell Phones Are Not Suitcases: Today's Reasonable Application of the Border Search Exception*, 52 Fordham Urb. L.J. 1085 (2025); Rebecca M. Rowland, *Border Searches of Electronic Devices*, 97 Wash. U. L. Rev. 545 (2019).

[13] *See* https://www.cbp.gov/document/directives/cbp-directive-no-3340-049b-border-search-electronic-devices. The CBP website also includes its most recent policy memo on the subject, CBP Directive No. 3340-049B (Jan. 28, 2026) (CBP Directive).

[14] *Id*.

[15] *Id*.

[16] *Id*.

[17] *Id*.

[18] *Id*. Current CBP policy limits inspections to the device itself and not information accessible via the device that is stored remotely. *See* CBP Directive, *supra*, ¶ 5.1.2.

[19] *Id*. In 2025, the ABA Center for Professional Responsibility updated its "Electronic Device Information" paper (ABA Paper) for attendees of the ABA annual meeting that year in Toronto. It is available of the ABA website. The ABA Paper discusses CBP policies, including those applicable to privileged documents on electronic devices. *See also* John Robert Schleppenbach, "With Summer Travel Season Approaching, Attorneys Should Take Precautions to Protect the Attorney Client Privilege," ABA Criminal Justice Section Newsletter, May 20, 2025 (available on the ABA website) (discussing the CBP policies noted in the context of electronic devices holding privileged material).

[20] *See generally* Anjli Raval, *Stricter US Border Controls Prompt Business Travel Rethink*, Financial Times, May18, 2025, available at www.ft.com (surveying business travel planning in the wake of increased border searches of electronic devices).

[21] The remedial protections for a search that violates stated CBP policy is a nuanced legal question beyond the scope of this column.

[22] *See, e.g.,* Brian X. Chen, *Fearing Border Searches on Your Phone? You Have Options*, N.Y. Times, May 13, 2025, at B4, available at www.nytimes.com; Heather Kelly, *How to Lock Down Your Phone If You're Traveling to the U.S.*, Washington Post, Mar. 27, 2025, available at www.washingtonpost.com; Sophia Cope, Amul Kalia, Seth Schoen, and Adam Schwartz, *Digital Privacy at the U.S. Border* (Dec. 2017), available on the Electronic Frontier Foundation website at www.eff.org; Lily Hay Newman and Matt Burgess, *How to Protect Yourself from Phone Searches at the US Border*, Wired, June 16, 2025, available at www.wired.com.

[23] *See, e.g.,* ABA Paper, *supra*; New York City Bar Formal Op. 2017-5, *supra*; Eva Novick, *Crossing International Borders*, 85 Or. St. B. Bull. 24 (July 2025).

[24] As collected in Note 5, *supra*, the ABA and the WSBA have a variety of resources available discussing protecting confidential information when accessing email and files remotely.

[25] *See* CBP Directive, *supra*, ¶ 5.1.2.

[26] The WSBA now offers a membership card with a personal photo. For more information, *see* https://www.wsba.org/for-legal-professionals/license-renewal/membership-records-and-services.

[27] *Id*., ¶ 5.2 (addressing CBP review and handling of privileged material).