ATTORNEY PROFESSIONALISM FORUM

Dear Forum:

On my return home from a summer vacation, I almost had a panic attack standing in line at U.S. Customs. The person in front of me was carrying a laptop with a flash drive and the customs agent instructed him to turn the laptop on, plug in the flash drive, and open certain documents on it. My laptop was in my bag hanging over my shoulder. I started thinking about what was on my laptop. I had been reviewing documents on a very sensitive deal between two well-known public companies that I am sure my client does not want anyone to know about. I am very careful about cybersecurity and the laptop required two-factor authentication to access any documents. But this border agent was directing the person to enter a password and show him information on the computer with a number of people in the immediate vicinity who could see the screen. Fortunately, I went through the checkpoint without having to even turn on my computer. But I travel frequently and I always bring my laptop with me. I know that a number of the attorneys at my firm regularly travel abroad and many of them take their laptops and phones with them. I am now very concerned about even carrying my laptop to the airport.

Under what circumstances can a customs agent demand to search through a passenger's electronic devices? Are there any limitations for what the customs agent can and can't search? Can they make copies of materials on my devices? Are there exceptions for attorneys who are carrying devices with sensitive or confidential client information? If an agent directs me to show them client information, should I explain to the agent that I am an attorney and carrying sensitive information that I cannot disclose?

If the agent insists on viewing the information despite my protests, is there anything else I can do? Am I violating any ethics rules by following the directions of the agent? Am I breaking any laws by refusing to comply with the agent? If an agent does review my devices and confidential or sensitive client information, what are my ethical responsibilities to my client? Does it matter if I have sensitive or confidential information from a potential client that has not yet retained me? What if the same issue arises with a customs agent from another country? Is there anything I should do to my devices the next time I travel abroad to prevent disclosure of client information?

Very truly yours,
Justin Cancun

Dear Justin:

Most attorneys are aware of the constant threat of cyberattacks and the potential harm to clients that can result from hackers gaining access to sensitive information. We have previously written about the use of Wi-Fi hot spots and have cautioned the bar about the need to protect client confidentiality when using smartphones and similar devices in public spaces, including airplanes. *See* Vincent J. Syracuse and Matthew J. Maron, Attorney Professionalism Forum, N.Y. St. B.J., May 2013, Vol. 85, No. 4. More recently, we looked at the issue from another angle, emphasizing the need to be vigilant about protecting client data and identifying attorney's best cybersecurity practices that will help minimize these threats. *See* Vincent J. Syracuse, Maryann C. Stallone, Richard W. Trotter, Carl F. Regelmann, Attorney Professionalism Forum, N.Y. St. B.J., June 2017, Vol. 89, No. 6. But your inquiry creates a whole new conundrum: An American government official may be demanding that you remove the very cybersecurity barriers you created to prevent an invasion of your client's confidential information. We understand your concern and near panic attack.

The inherent conflict between national security and an individual's civil rights during air travel is not new. For years, there has been a vigorous debate about the need and legality of numerous airport security measures including scanners, pat downs, forcibly removing passengers from airplanes, and even the removal of shoes. These measures, however, generally address concerns over immediate physical threats during travel or illegal physical activities such as drug trafficking and terrorist attacks. Your situation appears to be focused more on data suggesting to us that this border investigation may not have been focused on an immediate physical threat. While we have no way of knowing what information this border agent was seeking or what immediate threat he was working to thwart, scanning an individual's documents on computers in routine searches is invasive and should cause great concern to all attorneys traveling with their client's sensitive or confidential information.

The New York City Bar Association (NYCBA) Committee on Professional and Judicial Ethics recently addressed many of the issues that attorneys face in connection with international travel in Formal Opinion 2017-5. Under its policies, agents of U.S. Customs and Border Protection (CBP) are permitted

The Attorney Professionalism Committee invites our readers to send in comments or alternate views to the responses printed below, as well as additional hypothetical fact patterns or scenarios to be considered for future columns. **Send your comments or questions to: NYSBA, One Elk Street, Albany, NY 12207, Attn: Attorney Professionalism Forum, or by email to journal@nysba.org.**

This column is made possible through the efforts of the NYSBA's Committee on Attorney Professionalism. Fact patterns, names, characters and locations presented in this column are fictitious, and any resemblance to actual events or to actual persons, living or dead, is entirely coincidental. These columns are intended to stimulate thought and discussion on the subject of attorney professionalism. The views expressed are those of the authors, and not those of the Attorney Professionalism Committee or the NYSBA. They are not official opinions on ethical or professional matters, nor should they be cited as such.

to search electronic devices at the U.S. border when travelers enter or leave the United States including the information that is physically stored on the devices. NYCBA Comm. on Prof'l & Jud. Ethics, Op. 2017-5 at 2 (2017). This includes searching emails, text messages and electronically stored documents on devices carried by travelers. *Id.* According to its policies, CBP agents may demand disclosure of social media and email account passwords and seize devices during an inspection and they are not required to have a reasonable suspicion to do so. *Id.* Although the extent of such searches have been legally challenged and depends on the circumstances, a number of federal courts have held that reasonable suspicion is not needed for customs officials to search a laptop or other electronic device at the international border. *See* Robert T. Givens, *The Danger of U.S. Customs Searches for Returning Lawyers*, 30 GPSolo 3 (ABA 2013); *United States v. Levy*, 803 F.3d 120, 122 (2d Cir. 2015) (holding "[w]hen the evidence at issue derives from a border search, we recognize the Federal Government's broad plenary powers to conduct so-called 'routine' searches at the border even without 'reasonable suspicion that the prospective entrant has committed a crime.'") (citations omitted); *United States v. Arnold*, 533 F.3d 1003, 1009 (9th Cir. 2008). This suggests that CBP agents can search an electronic device of any traveler at random in their efforts to protect the borders and fulfill their customs, agriculture, and counterterrorism missions.

In 2009, the CBP issued CBP Directive No. 3340-049, *Border Search of Electronic Devices Containing Information*, which includes its guidelines for searching, reviewing, and retaining information obtained from border searches of electronic devices. (CBP Directive No. 3340-049, https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf). This directive includes a section addressing a CBP agent's special procedures for handling information claimed to be protected by the attorney-client or attorney work-product privileges:

> 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.

CBP Directive No. 3340-049 § 5.2.1. This directive also requires that CBP agents "encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure." CBP Directive No. 3340-049 § 5.2.3. Any privileged or sensitive information obtained in a search may only be shared with federal agencies that have mechanisms in place to protect such information under this directive. CBP Directive No. 3340-049 § 5.2.4. A CBP agent may only seize and retain an electronic device, or copies of information from the device, if "they determine that there is probable cause to believe that the device, or copy of the contents thereof, contains evidence of or is the fruit of a crime that CBP is authorized to enforce." CBP Directive No. 3340-049 § 5.4.1.1. In other words, by the terms of its own internal guidelines, the agents' authority to review information on electronic devices is broad even when an attorney specifically identifies that such information is protected or sensitive. It is likely that these policies may be applied differently from agent to agent. Further, it is possible that different CBP commissioners or administrative officials may have more expansive or restrictive interpretations of these guidelines or revise the guidelines. It certainly would not hurt to carry this directive with you when traveling in the event a certain agent is unfamiliar with these guidelines.

According to the Acting Commissioner of CBP, the CBP's authority to conduct border searches is limited to information *physically* residing on a device and does not extend to information located solely on remote servers. *See* June 20, 2017 *Due Diligence Questions for Kevin McAleenan, Nominee for Commissioner of U.S. Customs and Border Protection (CBP)* at 3, http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/170712-cpb-wyden-letter.pdf. The Acting Commissioner also stated that "CBP does not condition entry of U.S. citizens based on provision of a password, and has not denied entry into the United States to any U.S. citizen because of a refusal by such person to provide a password that would unlock their accompanying electronic device." *Id.* at 5. It is noted, however, that CBP Directive No. 3340-049 does not explicitly prohibit searching remote servers or prohibit denying entry for refusal to provide passwords. In any event, it may be advisable to store and access highly confidential client information through your firm's remote server, rather than saving documents to any local drives and email accounts or storing data on your portable electronic devices.

Under New York's Rules of Professional Conduct (RPC), you have a duty to protect your client's confidential information. As the NYCBA Committee on Professional and Judicial Ethics recently opined in NYCBA Formal Opinion 2017-5, this obligation applies while traveling abroad and carrying confidential client information and potentially undergoing a border search. Under RPC 1.6(c), which was recently amended, attorneys must "make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to," confidential information obtained from prospective, current, and former clients. RPC 1.6(c). This obligation is also implicit in the duty of competence under RPC 1.1. *See* NYCBA Formal Opinion 2017-5 at 4, citing ABA Formal

Op. 11-459 (Aug. 4, 2011). Comment 8 to RPC 1.1 specifically notes that in order "[t]o maintain the requisite knowledge and skill, a lawyer should . . . keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information." RPC 1.1 Comment [8]; *see* New York County Lawyers Association Professional Ethics Committee, Formal Op. 749 (2017) ("[a] lawyer's competence with respect to litigation requires that the lawyer possesses a sufficient understanding of issues relating to securing, transmitting, and producing [electronically stored information]. . . . If a lawyer is unable to satisfy the duty of technological competence associated with a matter, the lawyer should decline the representation."). "The duty to protect client confidences from 'unauthorized access' refers to access that is not authorized by the *client*." NYCBA Ethics Op. 2017-5 at 4, citing RPC 1.6 Comments [5] & [13]. Whether an attorney is making "reasonable efforts" to prevent unauthorized disclosure will inherently depend on the facts and the situation. Comment 16 to RPC 1.6, however, includes a nonexclusive list of factors to consider when making such a determination:

(i) the sensitivity of the information;
(ii) the likelihood of disclosure if additional safeguards are not employed;
(iii) the cost of employing additional safeguards;
(iv) the difficulty of implementing the safeguards; and
(v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or software excessively difficult to use).

RPC 1.6 Comment [16].

There is an exception to these rules which permits attorneys to disclose a client's confidential information in certain limited circumstances. RPC 1.6(b)(6) permits an attorney to reveal confidential information when required "to comply with other law or court order." RPC 1.6(b)(6). Comment 13 to RPC 1.6 is instructive in a border search situation: "Absent informed consent of the client to comply with the order, the lawyer should assert on behalf of the client nonfrivolous 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." Rule 1.6 Comment [13]; *see* NYCBA Ethics Op. 2017-5 at 8–9. Attorneys are not, however, required to risk violating their own legal or ethical obligations in seeking to challenge a law on behalf of their client. *See* NYSBA Comm. on Prof'l Ethics Op. 945 (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"); NYCBA Ethics Op. 2017-5 at 9.

The NYCBA Committee on Professional and Judicial Ethics has said that "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." NYCBA Ethics Op. 2017-5 at 9. We agree with that opinion, and likewise agree with their opinion that to be in compliance with this provision, attorneys must first take reasonable efforts to "dissuade border agents from reviewing clients' confidential information or to persuade them to limit the extent of their review" by informing the agent that they are attorneys, requesting that the devices not be searched or copied because the devices contain confidential or privileged information, and asking to speak to a superior officer if these requests are denied. *See id.* at 10. It is advisable to carry attorney identification with you when you travel abroad and be familiar with the CBP's authority and procedures including CBP Directive No. 3340-049. In addition, you should familiarize yourself with the laws of the country to which you will be traveling to determine the scope of materials that other country's border agents may search in accordance with their own laws. In the event that your device is searched or seized at the border, you have an obligation to promptly inform your clients, past clients, and potential clients of the information which the agent may have accessed. The RPC require that an attorney promptly inform the client of "any decision or circumstance with respect to which the client's informed consent . . . is required by these Rules" and to "keep the client reasonably informed about the status of the matter." RPC 1.4(a)(1)(i) and 1.4(a)(3); NYCBA Ethics Op. 2017-5 at 11. Comment 13 to RPC 1.6 also suggests that in the event of an adverse ruling after an attorney challenges the disclosure of confidential information, "the lawyer must consult with the client to the extent required by Rule 1.4 about the possibility of an appeal or further challenge . . . ." RPC 1.6 Comment [13]; NYCBA Ethics Op. 2017-5 at 11. Although informing your clients of the disclosure may be difficult, this will allow the clients to determine the best methods to prevent any possible damage from the disclosure. *See* NYCBA Ethics Opinion 2017-5 at 11.

So in the face of all of these rules, what should lawyers do to best protect their client's confidences? As an initial matter, lawyers traveling internationally with electronic devices should be mindful of Comment 16 to RPC 1.6 and the various factors discussed above when determining what level of protection is reasonably necessary to protect a client's confidential information. If you are working on very sensitive deals between well-known public companies, the first factor of RPC 1.6 Comment 16 suggests that you should be taking the strongest possible efforts to ensure that confidential information is not accessible in a routine border search. RPC 1.6 Comment [16]. In addition to encrypting devices with passwords as a basic precaution, some other methods to protect confidential information include using a blank "burner" phone or laptop and

then only accessing confidential information remotely from secured online locations. *See* NYCBA Ethics Op. 2017-5 at 7–8. To ensure that confidential information does not inadvertently get copied to the phone or laptop, software designed to securely delete information may be placed on the device, cloud service syncing should be turned off, web-based services should be signed out, and applications that provide local or remote access to confidential information should be uninstalled prior to crossing the border. *Id.* at 7. Lawyers should also avoid using removable storage devices to carry sensitive information and downloading the information they wish to protect on to a hard drive. Like it or not, if you are not sure how to implement these measures on your devices, and find it necessary to travel with highly sensitive confidential information, it may be advisable to contact a technology security consultant before you leave.

Sincerely,

The Forum by
Vincent J. Syracuse, Esq.
(syracuse@thsh.com)
Maryann C. Stallone, Esq.
(stallone@thsh.com) and
Carl F. Regelmann, Esq.
(regelmann@thsh.com)
Tannenbaum Helpern Syracuse & Hirschtritt LLP

QUESTION FOR THE NEXT ATTORNEY PROFESSIONALISM FORUM:

I'm currently representing a client whose honesty (or lack thereof) is becoming a problem. The litigation involves a dispute between siblings regarding a family business and, like many familial disputes, is highly contentious. I've always had a suspicion that given the opportunity, my client might try to pull something to get a leg-up on his siblings, but there haven't been any specific incidents that alarmed me until now. While preparing him for his deposition recently, the client all but told me that he intends to lie when asked a particular question by opposing counsel. Although I had my suspicions that something like this might happen given my client's personality and the nature of the dispute, I was still shocked. I always assumed that his brash statements and frequent outbursts were a product of his frustration with the whole case. I reminded the client that he would be testifying under oath during his deposition and warned him of the risks of perjury, but he was unfazed. He intends to go forward with his "strategy" during his deposition, and I'm not sure what to do. I know the client will decline any request I make to be relieved because it will be expensive for him to get a new attorney up to speed on this matter.

We have a status conference coming up before the court-appointed referee, and I'm considering moving to be relieved before the conference. Can I move to be relieved instead of notifying the court of the client's intent to lie at the deposition? If I am not relieved before the conference, do I have an obligation to tell the court referee what he said during our prep session even though my client hasn't actually committed perjury yet? What about opposing counsel? If I am obligated to inform the court referee and/or opposing counsel, are there any particular precautions I should take in order to safeguard my client's rights? In the event that I can no longer ethically represent this client, and am relieved as counsel, do I have to tell his next attorney of his apparent intention to lie during his deposition? On the off chance that the client does allow me to withdraw as counsel, if he decides to represent himself as a pro se litigant, do I still have an obligation to inform the court of his intent to lie under oath?

Another issue involving this troublesome client is also looming on the horizon. In the event that I am relieved as counsel, I'm certain that he will be furious with me. On prior occasions, he's been slow to pay his legal bills and has dissected many of my time entries, asking questions about every little task. I'm actually still waiting on him to pay his most recent bill, and I'm concerned that I'm not going to get paid after he finds out that I've made a motion to be relieved. If I do have to bring an action against this client to collect my fees, to what extent am I obligated to maintain attorney-client confidentiality especially in light of my reason for seeking to be relieved?

Very truly yours,
I. M. Forthright