Published on *The National Law Review* https://natlawreview.com

The Ever Thinning Right of Privacy at the Border—A Warning for Attorney Travelers.

Article By:

Eduardo Ayala Maura

It was March 2, 2020, at around five in the afternoon, right before the COVID-19 pandemic went out of control, and cities and states started to issue stay-at-home orders.

I had just gotten married to my wife on February 28 in Mexico. On our flight back we traveled with our family, around ten people in total. As we went through the automated customs system, my wife got an X in the receipt that the customs' machine sometimes gives you. Mine did not have an X but, since hers did, I accompanied her to the agent's kiosk that reviews receipts marked with Xs. When we got there, the agent reviewed her passport quickly, and told her that she would have to go through a secondary screening in what they call the "little room" or "el cuartico" in Spanish. As her husband, they let me go in with her.

We were in the "little room" for a few minutes, not too long. They reviewed her passport and then we were told to go to another place, following a long pathway full of orange plastic cones that took us to another agent, in a zone where there were scanning machines. The agent opened both of our bags, looked at them carefully, item by item, and then told us to sit and wait.

As we sat and waited for around twenty minutes, two agents came in and introduced themselves as being from the Investigative Unit at the Department of Justice. They showed us their badges. Without giving any details, they told us that they had orders from the agent-supervisor in charge to take our phones and laptops. My wife and I are both lawyers and, as such, reacted quite surprised, and quickly asked why. Both agents–one very polite, the other, not so much–told us that they could not tell us why they needed our phones and laptops, or what the whole thing was about. A back and forth, at times intense, ensued.

Our immediate reaction as lawyers was to say: "You don't have a right to do that. Please show us a warrant to search our phones or laptops." We additionally disclosed to them at that point that we were attorneys, and that our phones and laptops contained attorney-client sensitive information, and that such information does not belong to us but to the client. The polite officer did not say much. The not-so-polite officer said, essentially: "I don't care" and that "at the point of entry we have a right to inspect these things."

At the time, I did not know the law on this topic. As an immigration lawyer, I knew that non-citizens

seeking admissibility do not have a constitutional right to privacy. I thought that a different standard applied to U.S. citizens—which we both are. The agent seemed to disagree. I did not have time to research the law on my phone. The agents made us place our phones on the table, so we could not use them. The back and forth with the not-so-polite agent turned more intense. We managed to persuade him to let us use our phones to call our lawyers.

We called three lawyers. First, a good friend, Juan Carlos Gomez, an immigration law professor. He was of the view that if they were going to search our phones and laptops, they needed a magistrate's order or a warrant. I then called two good friends and excellent criminal attorneys. Both of them said something similar: "If they want to take it, they are going to take it, and there's not much you can do about it. You just need to make sure you are making it clear that you don't consent, and thus, anything inside cannot be used against you." All three attorneys told us that we did not have to provide the passwords of our phones and laptops; we just had to turn them in physically.

My wife and I were both unconcerned about ourselves. We really had nothing to hide but felt (1) that our right of privacy was being violated, and (2) that our clients' information was vulnerable. We both run small practices and take our phones and computers everywhere, as most lawyers do.

After some 60 minutes arguing with the agents, we agreed that we were going to wait for their supervisor to come see us before they took any of our laptops or phones. According to the not-so-polite agent, their boss had just been in a car accident and was going to take an additional hour. We said we would wait.

After around three hours since landing, tired, and with our family waiting outside, we said: "Let's just give it to them, let's not wait anymore." As we were about to turn in our phones, the agent-supervisor appeared. He was a nice man. We explained to him the situation, that we were attorneys, that our devices contained confidential attorney-client information, and that if he could give us any details about the topic of their investigation, we could cooperate and provide them with any necessary information. The agent-supervisor was polite, understood our position, and said not to worry about it, that he was going to let us go with our devices. We grabbed them and left.

To this day, we are not sure whether the agent-supervisor let us go because of the hassle of having to deal with two lawyers to obtain information that may not be all that valuable anyway, or if he let us go due to the attorney-client privilege concerns we shared with him.

Can U.S. border agents take an attorney's device which contains attorney-client privileged information?

The short answer seems to be yes.

The longer answer is laid out in the 2018 U.S Customs and Border Protection Directive No. 3340-049A (the "Directive").[i] Specifically, section 5.2 of the Directive, titled "Review and Handling of Privileged or Other Sensitive Material," addresses this issue head-on.

First, the information has to be "identified" or "asserted to be" protected by the attorney-client privilege. This burden is on the attorney. In other words, if you have attorney-client privileged information, it is your duty as a lawyer to make the claim.

Second, after there is a claim of attorney-client privileged information, the "Officer shall seek clarification, if practicable in writing, from the individual asserting [the] privilege as to specific files,

folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information."

Third, before any search may occur, where there is a claim of privilege, "the Officer will contact the CBP Associate/Assistant Chief Counsel (ACC) office." Then, in coordination with the ACC, the Officer "will ensure segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately."

Finally, at the completion of segregation and review, "unless any materials are identified that indicate threat to homeland security, copies of materials maintained by CBP and determined to be privileged will be destroyed, except for any copy maintained . . . for purposes of . . . a litigation hold."

In short, CBP officers may search a lawyer's phone, but they have to "segregate" the privileged information. How confident can you feel about border agents "segregating" and not looking at privileged material in searches they do out of your sight? I think we don't need to answer that question.

Can U.S. border agents access information remotely stored in "the cloud"?

The next question is how far they can search. We have not defined what a "device" is. Today, almost all smartphones are connected to "the cloud," which allows you to access vast amounts of information beyond what is stored in the actual physical device.

The Directive also addresses this. It specifically states that "[t]he 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." In fact, "Officers may not intentionally use the device to access information that is solely stored remotely." The Directive goes on to recommend that "Officers request that the traveler disable connectivity to any network . . . or where warranted . . . Officers will themselves disable network connectivity."

In other words, Officers can search your phone, but they cannot go into your Dropbox, iCloud, Google Drive or any other information that is stored in "the cloud" and that is accessed through internet connectivity. The question again becomes, how confident can you feel about border agents not accessing readily available information in Gmail, iCloud, Dropbox, and other cloud-based services? You really have no assurances that officers will not look at things you keep in "the cloud" that are so readily accessible. This underscores the importance of always having such applications logged out in your devices, but *especially* when you travel internationally.

Do you have to give U.S. border agents your password?

The Directive states that "[t]travelers are obligated to present electronic devices 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."

Thus, the Directive clearly says that you have to provide your password. However, it is unclear what remedy border agents have if U.S. citizens refuse to do so. In the case of non-U.S. citizens, it is clear that they could be denied admission into the country. It is highly unlikely, however, that a U.S. citizen attorney, making a claim of privilege, has to voluntarily disclose the password of the device that contains the privileged information. What happens if the attorney refuses to give his password? Will

he be arrested? What if he is arrested and still refuses to give his password? Will he be physically forced? It seems to be one of those situations where it will be difficult for U.S. agents to enforce. Of course, U.S. Customs is not completely without remedy, as the refusal to turn in the password will result in the impounding of the device and its opening using other electronic means.

What to do?

We will never know why they wanted our devices. Likely, it was something related to one of the hundreds of clients we have represented. But we do not know exactly which client or what the investigation was about.

What we do know now and learned from this experience is that we live in a world with increasingly fading privacy rights, and that we have to learn, as lawyers, to take necessary precautions to protect our clients' information. These precautions include traveling with devices that do not have access to cloud-stored information, such as Dropbox, Google Drive, Gmail, iCloud, or some legal software that relies on cloud computing. It is also important to travel with computers or phones that do not have anything in it that can be privileged. As seen above, even if the Directive says that the Officer has to "segregate" and not look at attorney-client privileged material, these searches happen out of your sight, and you have no control whatsoever over what the Officers look at. Until the Directive is challenged in court, Attorneys have to be extremely careful when they travel internationally.

---

[i] The legal authority or weight that the Directive carries is not the subject of this article; this article merely describes the current policy used by CBP in doing searches of attorneys' devices.

National Law Review, Volumess X, Number 119

Source URL:https://natlawreview.com/article/ever-thinning-right-privacy-border-warning-attorney-travelers