Keeping Your Data Safe Through US Customs

by Kenny Leckie of Traveling Coaches, Inc.

Are you familiar with the “broad search exception” of the U.S. Customs and Border Protection (CBP)? The CBP operates under the Department of Homeland Security (DHS), which has given it an exception from the rule requiring probable cause or a warrant before engaging in searches or seizure at international borders or international airports.

Let me explain why law firms need to familiarize themselves with the implications of this rule and how to continue protecting their clients during international travel.

Why Should You Care?
Lawyers and law firm personnel have an ethical responsibility to use technology competently when representing a client and to protect the confidentiality of that client’s information. This includes when passing through U.S. customs at the border. Simply claiming attorney-client privilege does not stop customs agents from potentially reading any document or information you may have.

What Is Being Done?
The American Bar Association (ABA) is working with the DHS to bring clarity to the options lawyers have at the border and recently received a revised directive from the CBP. It requires CBP officers to consult with CBP senior counsel when attorney-client privilege is asserted and details how privileged material is to be segregated and disposed of. This is an improvement over the original 2009 directive but still leaves us with a need to be aware and to plan for travel across U.S. borders.

What You Should Know
The ABA issued an electronic device advisory in January 2018 giving the following directives to lawyers:

» Determine which electronic devices contain attorney work product or privileged information and consider either leaving them at home or minimizing the number of devices with which you travel.

» Consider buying a disposable cellphone, inexpensive electronic device or fresh storage drive that carries only the information necessary for your travel period.

» Be familiar with the type and location of confidential information on any device with you. Also note that ordinary “delete” almost never fully removes data.

» Place all your devices in “airplane” mode as you approach a border inspection area, and fully power down or lock your electronic devices when appropriate.

» Have some form of identification ready showing that you are a legal professional, such as a work ID, your bar admission card or your business card.

» Be familiar with the requirements in your jurisdiction’s rules of professional conduct and how they dictate that you behave when approached with a request or demand for inspection, the expectations for how you will safeguard your clients’ information and the rules for notifying any clients whose information may have been revealed during a border search.

In addition, consider having the following:

» A firm policy for international travel that addresses where client information is stored.

» Special hardware with minimal data stored locally to be used for international travel.

» Client information placed in a hosted location that is accessed securely from the local machine but not resident on that machine.

Securing firm and client information is an issue all firms must address. The ethical obligation of keeping that information secure extends everywhere you may travel. Be informed, and prepare accordingly. P2P