LippesMathias LLP
ATTORNEYS AT LAW

The high-tech border: Risks and opportunities

By Elizabeth M. Klarin

March 14, 2018 | **IMMIGRATION**

U.S. Customs and Border Protection (CBP) is working to optimize resources using technology to streamline trade and individual border crossings. But in the new world of social media and virtual identities, technology is also enabling a deeper analysis impacting admissibility, eligibility for visas and qualification for other immigration benefits at the U.S. border. As America takes an increasingly protectionist stance on immigration, risks must be closely analyzed alongside opportunities in order to proactively and responsibly advise clients about what they may face when entering the United States.

Modern technology has been a great friend to cross-border businesses, enabling better, swifter communication; greater data accuracy and reporting; and more innovative methods and mechanisms for meeting customer or client needs. In the U.S. immigration space, technology is also streamlining certain processes, such as E-visa applications at U.S. consulates across Canada — many of which now require applicants to e-mail initial documents for analysis rather than using slower, more antiquated submission methods such as paper-based submissions by mail.

This has provided a great benefit to certain visa applicants by increasing their speed-to-ground to the U.S. However, technology is also being utilized by the U.S. government to create and drive transparent assessments of foreign national eligibility for immigration benefits — and catching some individuals off-guard when entering the United States.

In addition to assessing physical evidence of eligibility, border officers frequently utilize digital information to enforce a virtual border. One example of this is the recent increase in social media screening at the U.S.-Canada border. No one wants an off-handed comment via text about their nervousness waiting in line to cross the border — or additional detail about why they think they might have an issue crossing the border — to lead to heightened suspicion by a CBP officer and extensive questioning in the secondary inspection area. Likewise, people are often quick to update social media information on platforms such as LinkedIn with information on U.S. job postings they have been offered or approved for.

If your client needs but doesn't have a work visa for the U.S., and tries to cross the border with his or her status showing a U.S.-based job or residence, they are more likely than ever to be denied entry to the U.S. While some officers will simply turn clients away with advice to get an appropriate work visa, others may view in-person statements that conflict with social media or other online information as misrepresentation of material facts. Where this is the case, would-be entrants to the U.S. can expect a greater degree and intensity of questioning, at the very least.

While the driving objective behind social media screening initially was rooting out connections to terrorist organizations, it is becoming an increasingly commonplace practice to screen social media in determination of visa benefits. In essence, the cat is now out of the bag: expect to see widespread use of social media as a tool to screen applicants for any U.S. immigration-related benefit for ineligibility or inadmissibility.

It is important to recognize that according to CBP Directive 3340-049A published on Jan. 4, 2018, relating to border searches of electronic devices, CBP's policy directive is to "protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission." However, CBP officers must balance this against protecting the public from dangerous people and materials. Officers walk a daily line between supporting the global competitiveness of the U.S. and enabling legitimate trade and travel, and safeguarding America's borders by deterring, detecting and preventing threats to the U.S.

To help client prevent problems and cross smoothly into the U.S., awareness is key; CBP can search any device that may contain electronic or digital information — including computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players. A few tips to pass on to your clients include:

Disable network connectivity

According to CBP policy, officers should only be examining 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."

"Privileged" information does not necessarily mean it cannot be examined

W hile CBP is required in some instances to segregate "privileged" information — such as attorneyclient work product or information protected by attorney-client privilege — they may be able to examine this information to determine whether any of it indicates an imminent threat to homeland security. If your client is concerned about the privacy of his or her information, the best policy is not to have it on any device he or she is travelling with.

Be respectful

B order searches and questions arising from technological triggers can be frustrating, time consuming and feel unnecessary or hostile. However, becoming aggravated or hostile in response to questions or actions by officers will never result in a positive outcome. Advise your clients to be respectful and patient.

Seek assistance ahead of time

I f your client feels that they may have reason to worry, advise them to reach out to an immigration lawyer ahead of time rather than waiting until an officer denies them entry. Having a denial on their record can make any immigration process more complicated, particularly where notes have been entered into CBP's system that may create concern for future officers assessing the individual's eligibility to enter the U.S.

Disclaimer: *The information in this post is provided for general informational purposes only, and may not reflect the current law in your jurisdiction. No information contained in this post should be construed as legal advice from our firm or the individual author, nor is it intended to be a substitute for legal counsel on any subject matter. No reader of this post should act or refrain from acting on the basis of any information included in, or accessible through, this post without seeking the appropriate legal or other professional advice on the particular facts and circumstances at issue from a lawyer licensed in the recipient's state, country or other appropriate licensing jurisdiction.*