MOSES & SINGER LLP

Client Alert January 2018

New Rules for Electronic Device Border Searches: Are Attorneys and Clients Prepared?

By: Devika Kewalramani, Gregory S. Shatan, Blaze D. Waleski and Tyler E. Margolis

Imagine that you are traveling back to John F. Kennedy Airport from an overseas vacation, when a United States Customs and Border Protection ("CBP") officer demands that you unlock or unencrypt your smartphone, tablet or computer full of client data and hand it over for a search. How do you react - do you refuse to comply with the CBP officer or do you willingly turn over your devices? You might be thinking, "How can CBP do this?" "Do I have to comply?" "What can I do to stop this?"

On January 4, 2018, the CBP released Directive No. 3340-049A ("CBP Directive") regarding U.S. border searches of electronic devices belonging to any traveler - U.S. Citizens, green card holders or foreign nationals – entering or exiting the country. The new CBP Directive supersedes its Directive No. 3340-049 issued in 2009 ("Prior Directive"), providing federal regulatory authorities with sweeping legal authority to search, review, retain and share information contained in computers, tablets, removable media, disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic or digital devices that belong to a traveler, in some instances without a warrant, at U.S. border crossings.

These new rules follow the U.S. government's increasingly tighter border control policies which have resulted in a significant surge in border searches of electronic devices by the CBP. According to CBP statistics issued in January 2018, the agency conducted 30,200 inbound and outbound border searches of electronic devices in 2017, significantly greater than the 19,051 devices searched in 2016.

Border searches of electronic devices may include "searches of the information stored on the device when it is presented for inspection or during its detention by CBP." The search will include "an examination of only the information that is resident upon the device and accessible through the device's operating system or though other software, tools, or applications." CBP officers are not permitted to intentionally use the device to access data that is solely stored remotely. To avoid accessing or retrieving such data, CBP officers may ask the traveler to disable connectivity to any network (e.g., placing the device in airplane mode), or where warranted by national security concerns, they will disable network connectivity. CBP officers are required to ensure that they make no changes to content on the device during the course of a search.

The CBP Directive distinguishes "basic" searches, conducted with or without suspicion, where a CBP officer may examine an electronic device and review and analyze information encountered at the border, from "advanced" searches, which require "reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern." During an "advanced" search, a CBP officer may connect external equipment to an electronic device, "not merely to gain access to the device, but to review, copy, and/or analyze its contents." Further, the CBP Directive proscribes that travelers "are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents." For example, if a traveler hands over a cell phone with a passcode or encryption, he or she must unlock the phone or decrypt data; otherwise the CBP officer could detain or seize the device, or prohibit travel with the device. This could lead to delay in travel and may even effectively deny entry to or exit from the United States.

Suppose the traveler subject to a border search is a lawyer whose smartphone, tablet and computer contain highly sensitive and confidential client information? What should the lawyer do? Violate the law by refusing inspection of his or her electronic devices or breach his or her duty of confidentiality and waive attorney-client privilege by handing them over? The ethical rules governing a lawyer's conduct generally prohibit a lawyer from knowingly disclosing confidential client information without client consent or unless specifically excepted by the rules, or when reasonably necessary to comply with law. Lawyers are ethically obligated to make reasonable efforts to prevent unauthorized access to confidential client information.[1]

Guidance on how to review and handle privileged or other sensitive material is outlined in the CBP Directive. Initially, the CBP officer is directed to "seek clarification, if practicable in writing, from the individual asserting this privilege . . . that may assist CBP in identifying privileged information." Before searching any materials over which privilege is asserted, the CBP officer is instructed to contact the CBP Associate/Assistant Chief Counsel office, who will coordinate with the U.S. Attorney's Office as needed, to ensure steps are taken to properly segregate any privileged material from other information that is examined. Unless any materials are identified that pose an imminent threat to national security, copies of any privileged materials maintained by CBP will be destroyed. The CBP Directive treats "business" or "commercial" information contained in electronic devices as "business confidential information" that will be protected from unauthorized disclosure.

In addition, the CBP Directive includes detailed procedures on detention of a device (not to exceed five days in normal circumstances); retention, sharing, safeguarding and destruction of information; and related reporting requirements.

Previously, in May 2017, the American Bar Association ("ABA")[2] raised concerns with the Department of Homeland Security ("DHS") regarding the standards contained in the Prior Directive that allowed CBP officers to search and review a lawyer's electronic devices containing client confidential data at U.S. border crossings, without any showing of reasonable suspicion of wrongdoing. The ABA asked the DHS for a revised directive on the procedures for border search and seizures of lawyer devices. In July 2017, the New York City Bar Association's Committee on Professional Ethics issued formal opinion 2017-5 (2017) ("Opinion")[3] setting out the ethical duties of a lawyer when crossing a U.S. border with confidential or privileged client data. The Opinion offers guidance to lawyers at three junctures: prior to crossing the U.S. border, at the border where the CBP officer seeks review of data on the attorney's device, and after the border search, as follows:

- Before crossing the border, the Opinion suggests taking reasonable steps in advance to avoid disclosing confidential client data if a CBP officer asks to search the lawyer's device, such as: deleting confidential files and securely backing it up prior to crossing the border, using a blank "burner" phone or laptop, turning off syncing of cloud services, signing out of web-based services, and/or uninstalling applications providing local or remote access to confidential data.
- At the border crossing, the Opinion suggests undertaking reasonable efforts to dissuade CBP officers from reviewing client data or persuade them to limit the extent of their review, such as: informing them that the device or files contain privileged or confidential data, requesting that such materials not be searched or copied, asking to speak to a superior officer, and to add credence to the claim of privilege, carrying and presenting, if needed, some form of attorney identification, e.g., court-issued attorney ID, proof of bar membership or a business card.
- After a border search or seizure, the Opinion suggests that the attorney must notify affected clients of what occurred and the extent to which client data may have been reviewed or seized, in compliance with the general duty to communicate with clients under Rule 1.4[4] so that clients have the opportunity to consider their options and take any necessary action.

The new CBP Directive will not stop lawyers and clients from crossing U.S. borders for business or leisure trips. However, it should prompt them - and their employers and organizations - to take a hard look at what policies and practices would reasonably protect client data consistent with their fiduciary and ethical responsibilities, while avoiding undue delay or unpleasantness at the border. To avoid unintended consequences, complications and even confrontations, successful policies will need to be tailored to the needs and circumstances of each firm or company, with sufficient flexibility to cover different situations. Employers will need to develop and implement these policies – and make sure that clients and counsel with access to the same data do so as well – long before planning that next trip across a U.S. border. If firms and companies don't focus on this issue, lawyers and clients could find themselves trapped in the terminal or left without their own devices.

---

[1]See Rule 1.6 of the New York Rules of Professional Conduct. This rule is similar to the ABA Model Rules of Professional Conduct that have been adopted by most U.S. jurisdictions.

[2]See the ABA's letter dated May 5, 2017 to the DHS: https://www.americanbar.org/content/dam/aba/images/government_affairs_office/attyclientprivissue(bordersearchesofattorneydevices,abalettertodhs,finalversion,may5,2017).pdf

[3]New York City Bar Association's ethics opinion dated July 25, 2017 references the Prior Directive.

[4]See Rule 1.4 of the New York Rules of Professional Conduct. This rule is similar to the ABA Model Rules of Professional Conduct that have been adopted by most U.S. jurisdictions.

MOSES & SINGER LLP

Since 1919, Moses & Singer has provided legal services to diverse types of businesses and high-net-worth individuals. Among the firm's broad array of U.S. and international clients are leaders in banking and finance, entertainment, media, real estate, healthcare, advertising, and the hotel and hospitality industries.

In a world of giant, multi-office law businesses assembled by mergers, built on associate leverage and driven by billable hour quotas, the needs of clients can get lost. Moses & Singer offers a difference. That difference is the attention of leading practitioners-partners in the firm-with the experience and knowledge to provide our clients creative, cost effective, result-oriented representation. The direct involvement of our partners means aggressive, focused problem solving. The firm's attorneys concentrate their practices in the following areas:

- Accounting Law Practice
- Advertising
- Asset Protection
- Banking and Finance
- Business Reorganization, Bankruptcy and Creditors' Rights
- Corporate/M&A
- Corporate Trust and Agency
- Employment and Labor
- Entertainment
- Family Office
- Global Outsourcing and Procurement
- Healthcare
- Hospitality, Food Service and Restaurants
- Income Tax
- Intellectual Property
- Internet/Technology
- Legal Ethics and Law Firm Practice
- Litigation
- Matrimonial and Family Law
- Privacy
- Private Funds
- Promotions
- Real Estate
- Securities and Capital Markets
- Securities Litigation
- Trusts and Estates
- White Collar Criminal Defense and Government Investigations