IMMIGRATION LAW AND GLOBAL SERVICES

January 2018

Are Your Personal and Corporate Electronic Devices and Data Safe When Traveling?

On Jan 4, 2018, U.S. Customs and Border Protection (CBP) issued a guidance, Directive 3340-049A, governing Border Searches of Electronic Devices. The purpose of this directive is to assure that the "authority for border search of electronic devices is exercised judiciously, responsibly and consistent with public trust." The business community has viewed these searches as a cause of anxiety and concern for all employees regardless of status, that require due diligence and forethought.

HIGHLIGHTS

- There is no right to counsel at a U.S. port of entry regardless of status
- CBP / ICE agents can lawfully search data stored on electronic devices.
- Employers must develop policies on travel and use of electronic devices containing sensitive or privileged data.

Over the past several years, CBP and U.S. Immigration and Customs Enforcement (ICE) have increased inspections of data stored on electronic devices at borders and other ports of entry when arriving to or departing from the United States. Officers may request to review data stored on electronic devices. They may also ask the device owner to unlock password protected or encrypted devices, and even passwords to social media. Data on devices may be viewed or copied by government agents and devices that cannot be accessed or show evidence of a violation or crime may be confiscated temporarily or permanently. This is not limited to foreign nationals; it has been applied to U.S. citizens and permanent residents as well.

The frequency of these searches increased dramatically. In 2017, CBP performed 32,000 border searches of inbound and outbound travels with electronic devices compared to 19,051 in 2016 – a 60% plus increase. In fact, these searches are not limited to departing and arriving passengers on international flights – they may occur in some circumstances throughout the country.

The directive provides the following guidance to the field on border searches of electronic devices:

- Border searches will only examine information that is stored locally on the device.
- Officers may only perform an advanced search if there is reasonable suspicion or for national security reasons.
- Officers must follow specific procedures when handling privileged or business-sensitive information.

How should companies handle confidential information on employee devices while traveling? How do professionals, like lawyers, doctors, accountants, financial advisers, etc., protect confidential client information on these devices?

Key issues to consider and examine are:

- **There is no right to legal counsel at a U.S. port of entry and searches are legally permitted as a sovereign right**. It is critical to develop a plan now, working with legal counsel familiar with the law and directive.
- **Learn how to handle law enforcement requests.** These requests could be related to business-sensitive and privileged (attorney-client) or confidential private information.
- **Develop a policy.** Now more than ever, it is critical to develop a plan and policies to protect confidential company and client information on electronic devices while traveling. Review and update policies relating to marking, storing, and handling sensitive business or client's protected information when traveling internationally.
- **Provide employees with resources.** Coordinate with legal counsel to provide contact information when employees travel internationally and domestically.

To obtain more information, please contact the Barnes & Thornburg Labor & Employment attorney with whom you work, or Mariana Richmond at 317-231-7476 or marianna.richmond@btlaw.com; Mercedes Badia-Tavas at 312-214-8313 or mbadiatavas@btlaw.com; Jeff Papa at 317-231-7507 or jeff.papa@btlaw.com.

Visit us online at www.btlaw.com or on Twitter @BTLawLE, and don't forget to bookmark our blogs at www.btlaborrelations.com and www.btcurrents.com.