crowell moring

CLIENT ALERT

Searches of Electronic Devices at the Border Increase Nearly 60 Percent; DHS Issues Updated Border Search Policy

Jan.08.2018

On Friday, January 5, 2018, U.S. Customs and Border Protection (CBP), a component of the Department of Homeland Security, released the fiscal year (FY) 2017 statistics relating to warrantless searches of electronic devices at the border; they show a significant increase in border searches—30,200 in FY 2017, up from 19,051 in FY 2016 (which was itself up from 8,503 in FY 2015). CBP also released a new policy directive governing such searches, replacing guidance from 2009. The updated policy clarifies the standard operating procedures for searching, reviewing, and retaining information found on electronic devices. Key components of the new policy include:

- **Border searches will only examine information that is stored locally on the device**. Officers are instructed to ensure the device is in "airplane mode" or a similar offline state to avoid accessing information that is solely stored remotely, such as on a cloud-based service.
    - *Impact*: This policy, previously announced in 2017, appears to limit access to information stored solely in the cloud and not downloaded to the electronic device. It may include information and private messaging on social media platforms, data backed up to the cloud, and web-based email services if messages are not downloaded to the electronic device.
- **Officers may only perform an advanced search if there is reasonable suspicion or for national security reasons**. The new directive distinguishes between a "basic" and an "advanced" search. A basic search is a cursory search of the device, which most courts have said does not require any suspicion or cause. An advanced search is any search in which an officer connects external equipment to an electronic device to review, copy, and/or analyze its contents. Officers, however, may only perform an advanced search if there exists reasonable suspicion of unlawful activity or a national security concern arises. Officers are also required to obtain relevant supervisory approval for an advanced search.
    - *Impact*: This change appears to generally apply nationwide a reasonable suspicion standard to perform an advanced search, which conforms to heightened search requirements set by courts in some jurisdictions like the Ninth Circuit. *See United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013).
- **Officers must follow specific procedures when handling privileged or business-sensitive information**. The new directive outlines specific procedures if officers encounter or are informed of information protected by the attorney-client privilege or attorney work product doctrine. In such cases, the officer must: (1) seek clarification from the individual as to the specific information protected by either doctrine; and (2) contact the CBP Associate/Assistant Chief Counsel office to ensure the segregation of any privileged material to ensure appropriate handling. Relatedly, officers who encounter business-sensitive information are required to treat such information as confidential and protect it from unauthorized disclosure. The policy does not outline any special process or protection for journalists' materials or medical records.
    - *Impact:* The new policy does not prevent officers from searching protected information. Rather, it sets up a specific process for officers to follow, which may include employing a filter or taint team to review attorney-

client information or attorney work product. The bottom line is that attorney-client, business and other sensitive information stored in an international traveler's electronic device remains subject to search.

- **Officers may ask travelers to unlock electronic devices**. Today many devices are passcode protected or otherwise encrypted. An officer may request the individual's assistance to access the device, *i.e.,* ask them to unlock the device. If officers are unable to conduct their search due to a locked device, they are expressly permitted to detain the device (subject to time and supervisory approval limitations) to complete their inspection.
    - *Impact*: If a device is password-protected and the traveler chooses not to unlock it, customs officers may detain the device to determine whether they will allow its entry into the United States. Officers might also ask the individual questions about why they will not unlock the device.
- **Officers must safeguard data during storage and conveyance**. The new directive requires that officers appropriately safeguard information that is retained, copied, or seized, including keeping materials in locked cabinets or rooms, documenting and tracking copies, and generally safeguarding materials during conveyance.
    - *Impact*: The requirements to safeguard data seized by law enforcement sets some baseline requirements for the government's protection of that information, but the policy also makes clear that relevant data can be used and shared in the course of a government investigation.

The updated policy reflects how law enforcement continues to grapple with the impact of new technologies in the digital age while attempting to balance their law enforcement mission with individual privacy rights. Businesses should reflect on the new guidance as they continue to operate in a global environment and consider:

- Reviewing and updating policies relating to marking, storing, and handling sensitive business or attorney-client protected information when traveling internationally.
- How employees should deal with law enforcement requests related to business sensitive and attorney-client information.
- Providing employees with contact information for counsel when traveling internationally.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Kelly T. Currie
Partner – New York
Phone: +1 212.895.4257
Email: kcurrie@crowell.com

Christopher D. Garcia
Associate – Washington, D.C.
Phone: +1 202.688.3450
Email: cgarcia@crowell.com