CLIENT ALERTS & INSIGHTS

U.S. Customs and Border Protection Updates Directive on Searches of Electronic Devices

APRIL 4, 2018

Authors: H. Alan Rothenbuecher

U.S. Customs and Border Protection ("CBP") recently updated its 2009 directive pertaining to border searches of electronic devices. The Supreme Court of the United States has deemed warrantless searches by CBP legal and "reasonable" in light of national security concerns. With the advent of this digital age, CBP has now expanded its directive to include searches of electronic devices, which include password-protected laptops, phones, and other handheld devices.

The updated directive also states that travelers shall "present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents." Therefore, CBP officers may request that travelers enter any passwords or biometric data to allow for device inspection. While U.S. Citizens cannot be denied entry to the United States for refusing to provide a password, a CBP officer may detain the electronic device for further inspection. Non-citizens that refuse to allow inspection may be denied entry or face complicated questioning.

In expanding the scope of the directive, CBP did recognize that a search of an electronic device should only encompass information stored on the device itself. Information stored on cloud-based platforms should not be included in a CBP search. The directive further distinguishes between "basic" and "advanced" searches. "Advanced" searches, which require the use of external equipment to review, copy, or analyze device contents, are only permitted when there is reasonable suspicion of unlawful activity or a national security concern.

Additionally, attorney-client privileged material is remains subject to heightened protections. When an individual asserts this privilege, the CBP officer should request clarification as to specific files, file types, folders, or categories of information that may be privileged. CBP then utilizes "Filter Teams," comprised of legal and operational personnel, to segregate the privileged information. But because such Filter Teams are few and far between, a traveler asserting the attorney client privilege will likely have his or her device detained. Upon completion of the inspection, copies of any materials maintained by CBP and determined to be privileged will be destroyed.

While the CBP still only examines 0.01% of travelers' electronic devices, the consequences of being selected for such an inspection are significant. Individuals with any data stored on their electronic devices that is sensitive or privileged, should consider taking steps to protect against device seizure and/or information disclosure. Accordingly, travelers should consider:

- Using a temporary or travel laptop, forensically cleared of local documents and privileged information;
-

Using a temporary or travel mobile phone - business calls may be forwarded from an office number to the mobile phone;

- Utilizing software and tools housed on the internet;
- Turning off devices at least five minutes before reaching an inspection point to avoid access to Random Access Memory;
- Backing up and deleting sensitive data in advance of reaching an inspection point;
- Utilizing a separate user account and/or e-mail account for sensitive information - if possible, removing the accounts from device in advance of reaching an inspection point;
- Using strong encryption and complex passwords;
- Utilizing two-factor authentication;
- Utilizing “private browsing” features and clearing search histories and cookies;
- Partitioning and encrypting hard drives;
- Protecting the FireWire data port; and
- Wiping smart mobile devices remotely.

The updated directive is available at:

https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Sea

If you have any questions on this topic, please contact a member of Benesch's Immigration Practice Group:

H. Alan Rothenbuecher at arothenbuecher@beneschlaw.com or 216.363.4436

Linda Gemind at lgemind@beneschlaw.com or 216.363.4609

Margarita S. Krncevic at mkrncevic@beneschlaw.com or 216.363.6285

Rick Hepp at rhepp@beneschlaw.com or 216.363.4657