CBP Announces New Border Search Policy

On January 4th, U.S. Customs and Border Protection ("CBP") issued a Directive to standardize procedures its officers' use during border searches, which include searches of all persons entering the United States through airports. The CBP claims plenary authority to conduct searches of electronic devices under its recognized authority to conduct "routine searches of the persons and effects of entrants [into the United States, which] are not subject to any requirement of reasonable suspicion, probable cause, or warrant."[1] The Directive sets forth the scope and extent of the searches that CBP can perform of electronic devices such as laptops, tablets, and mobile phones.

Entrants into the U.S. should be particularly aware of Section 5.2 of the Directive, which covers privileged material. The rules governing privileged material were included in the Directive in response to concerns in a letter from the American Bar Association. Section 5.2 sets procedures for CBP officers to follow when encountering material asserted to be protected by the attorney-client privilege or the attorney work product doctrine. Officers should first clarify with the owner of the electronic device which files are specifically protected by a privilege. Officers cannot search any privileged material without first contacting the CBP Chief Counsel office and establishing a Filter Team, composed of both legal and non-legal CBP personnel, to assist in segregating privileged materials from other files.

Searches can be basic or advanced. Basic searches are those conducted without the aid of external equipment CBP personnel use to review, copy, or analyze the device's contents. They should be conducted in the presence of the device's owner unless there are safety concerns rendering the owner's presence inappropriate. Advanced searches are searches requiring external equipment to review the device. They require reasonable suspicion of unlawful activity. It appears that this heightened threshold for more extensive searches is in response to the Court of Appeals for the Ninth Circuit's ruling in *United States v. Cotterman*, which held that border searches involving "comprehensive and intrusive" forensic searches of laptops cannot be carried out absent reasonable suspicion.[2]

Once CBP officers complete their search of an electronic device, they must destroy any privileged materials that they have copied. Business or commercial information should be treated similarly and protected from unauthorized disclosure. Troublingly, the Directive does not appear to preclude CBP review of information identified as sensitive, but instead merely provides that CBP shall not continue to store such information after the conclusion of the search, with notable exceptions for materials posing an imminent

[1] *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).

[2] 709 F.3d 952, 962 (9th Cir. 2013) (en banc).

threat to homeland security or copies maintained solely for the purposes of complying with a litigation hold or other legal requirements.

Business travelers who are stopped by CBP while entering the United States should know these requirements and ensure that CBP officers follow them. Entrants should insist that any basic searches be conducted in their presence. They should tell the CBP officers that they do not want the device to leave their sight. And they should call a lawyer if necessary to ensure compliance with the Directive. In addition, entrants are entitled to know the purpose and authority for a border search, as well as means to report concerns and seek redress from the CBP. CBP officers are entitled to detain devices for up to five days. If a device is detained, entrants should make sure they receive a receipt from border agents.

Entrants should also advise CBP personnel performing the search of any privileged, confidential, or trade secret information contained on the device or devices subject to search. If CBP personnel fail to do so of their own accord, entrants should insist that the office of the CBP Chief Counsel be notified and that the appropriate Filter Team be assembled to ensure protection of sensitive information. In order to facilitate the protection of sensitive information, it may prove helpful to segregate privileged, confidential, or trade secret information to a single, clearly-labeled folder or directory when traveling internationally, so that the information can be easily identified to CBP and treated in accordance with the Directive.

Because the Directive requires entrants to provide login and password information, encryption or password protection will not be a useful tactic for protecting sensitive information. One possible method of protection is not to store any privileged materials on your electronic devices at all. Retaining privileged documents in a password-protected secure cloud server or a remote file-saving system ensures that CBP, when searching your device, cannot access any protected material. And Section 5.1 permits officers to search "only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications." Officers cannot access information that is solely stored remotely, and must either enable airplane mode or disable internet connectivity before searching a device. Entrants should themselves ensure their devices are in airplane mode, or insist that CBP personnel disable their devices' connectivity before conducting a search. This both protects remote files and prevents downloading of harmful malware. But note that any remotely stored information that is synced with the device's operating system is accessible; only remote information that is not downloaded will be protected.

If asked for their passcode or encryption key, entrants should enter the information themselves, instead of divulging it to CBP officers. If an entrant refuses to provide this information, a CBP officer may detain the device. Entrants should also change passwords as soon as their device is returned.

About Curtis

Curtis, Mallet-Prevost, Colt & Mosle LLP is a leading international law firm. Headquartered in New York, Curtis has 17 offices in the United States, Latin America, Europe, the Middle East and Asia. Curtis represents a wide range of clients, including multinational corporations and financial institutions, governments and state-owned companies, money managers, sovereign wealth funds, family-owned businesses, individuals and entrepreneurs.

For more information about Curtis, please visit www.curtis.com.

Attorney advertising. The material contained in this Client Alert is only a general review of the subjects covered and does not constitute legal advice. No legal or business decision should be based on its contents.

Please feel free to contact any of the persons listed below if you have any questions on this important development:

Jonathan J. Walsh
Partner
jwalsh@curtis.com
New York: +1 212 696 8817

Michael J. Moscato
Partner
mmoscato@curtis.com
New York: +1 212 696 6946

Edward F. Combs
Associate
ecombs@curtis.com
New York: +1 212 696 6069