Frequently Asked Questions: Electronic Device Searches at U.S. Border

U.S. Customs and Border Protection (CBP) is authorized to conduct searches at U.S. ports of entry. These searches do not require CBP to possess a warrant or probable cause. Under this authority, CBP may examine electronic devices such as laptops, phones, tablets, USB drives, external hard drives, or other digital storage media. CBP may ask any travelers to provide these devices before entry to or departure from the United States.

For non-citizens, deciding to not comply with CBP requests may result in refused entry to the United States. For all travelers, CBP may also seek to confiscate devices without a pre-determined timeline for return.

Although passwords and multi-factor authentication are best practices for security, CBP may request this information at the port of entry to conduct searches. We recommend non-citizens check in with their employer and review their employer's policies regarding the carrying and use of employer provided electronic devices during travel.

The following provides helpful guidance regarding these potential searches, what may be requested, and what impacts may result upon entry to the United States.

Why does CBP search electronic devices?

In general, CBP conducts these searches to determine whether a device contains digital contraband, terrorism-related information, or information relevant to the traveler's admissibility.

Who can be searched?

All travelers regardless of citizenship, baggage, and merchandise arriving in, or departing from, the United States may be inspected by CBP.

Are there multiple types of searches?

Yes, CBP conducts basic searches and advanced searches of electronic devices.

What are basic searches?

Basic searches generally involve manual review of electronic devices without the assistance of external equipment.

What are advanced searches?

Advanced searches generally involve a CBP officer connecting external equipment to the traveler's device to gain access and to review, copy, and analyze its content.

When can CBP connect their own search devices to my device?

CBP's authority to conduct searches at the border is broad. However, to conduct an advanced search, CBP generally must have reasonable suspicion of a violation of law enforced or administered by CBP or a national security concern.

What may CBP request at a port of entry?

During travel to the United States, CBP may request travelers to hand over for search any electronic devices, including laptops, phones, tablets, USB drives, external hard drives, or other digital storage media. In doing so, CBP may:

- Request the traveler to unlock their device(s) and provide passwords;
- Access emails, messages, call logs, social media accounts, photographs, files, and cloud-stored content to which the device is already synced;
- Review travel-related documents, financial records, and professional correspondence; and/or
- Conduct forensic imaging by connecting their own devices.

While CBP policy states that privileged or sensitive materials (e.g., attorney-client communications, proprietary business information, etc.) must be handled with care, officers may still view such information unless specific procedures are invoked.

What options do I have in response to these requests?

While interacting with CBP, we recommend you comply with the officer's requests to the extent possible. Travelers should keep up to date with their employer's encryption and data privacy policies related to their employer provided electronic devices, and be aware of complying with these policies during any interactions with CBP at entry to the United States.

What procedures relate to confidential information?

CBP's current policies provide specific processes for privileged and other sensitive material. In particular, data that is identified or asserted to be protected by attorney-client privilege, for example, require additional screening procedures from the reviewing officer. These reviewing procedures may include requesting the traveler to clarify which files, file types, folders, names, contact information, or other particulars may define the sensitive information. Prior to searches of these sensitive materials, the reviewing officer generally is required to escalate the issue within CBP to initiate a process of segregating files between protected files and unprotected files.

Importantly, business and/or commercial information that is identified during a search is to be treated by the CBP officer as business confidential information and to be protected from unauthorized disclosure. This information may be restricted from search by the Trade Secrets Act, the Privacy Act, and other laws and CBP policies, as well.

Frequently Asked Questions: Social Media and Your Immigration Applications

The U.S. immigration agencies are currently at different stages of adding requests for social media information on various benefits applications. The U.S. Department of State (DOS) requires this information on most visa applications submitted to U.S. consulates, including the DS-160. The U.S. Department of Homeland Security (DHS) is also currently considering a new proposed rule to add requests for social media information to in-country applications such as the Form I-485, Application to Adjust Status (green card application).

As a reminder, foreign nationals should be conscious and mindful of their presence on social media. The government can and does request and review social media accounts and posts as part of immigration benefits applications. Making your accounts private and remaining thoughtful about the content you post are a few best practices to consider.

The following provides helpful reminders regarding how your social media presence may impact your immigration journey.

Why is this information requested?

The U.S. government utilizes collected social media information to heighten the vetting process for visa applicants. By reviewing applicants' online presence, consular officers aim to identify (1) potential discrepancies in the information provided in the DS-160 online application, such as different employment history information in an online profile versus the information submitted on the DS 160 application or an immigration benefits application, and (2) potential security concerns, such as involvement in activities that could pose a threat to the United States.

How could my visa application be impacted by my social media presence?

Applicants' online activities are subject to examination, and content deemed to be of a national security concern, inconsistent with the United States's public policy positions, or contradicting information provided in the DS-160 online visa application form can lead to visa and immigration petition denials, as well as revocations of already issued visas or immigration benefits.

Failure to disclose required social media information, or providing false identifiers, may have similar consequences, as such conduct may be considered a misrepresentation. A misrepresentation on a government form can have significant, long-term, and/or permanent consequences on someone's immigration status and/or ability to enter the United States. Applicants are advised to be thorough and truthful in reporting their social media usage to avoid potential penalties. If you have any questions, we recommend you speak to immigration counsel to address your questions.

When am I required to disclose my social media information for immigration purposes?

Currently, the U.S. government requires most visa applicants to disclose their social media identifiers from the previous five (5) years on their visa application forms, specifically the DS-160 (nonimmigrant visas) online application. DHS is also considering similar requests be included on applications submitted to U.S. Citizenship and

Immigration Services, such as naturalization (citizenship), adjustment applications (green card), travel authorization (advanced parole) applications, among others.

What information do I need to disclose?

The U.S. government requests all social media usernames or handles used **during the past five (5) years**. The application form lists specific platforms, including **but not limited to**:

- Ask.FM
- Douban
- Facebook
- Flickr
- Google+
- Instagram
- LinkedIn
- MySpace
- Pinterest
- QZone (QQ)
- Reddit
- Sina Weibo
- Tencent Weibo
- Tumblr
- Twitter
- Twoo
- Vine
- VKontakte (VK)
- Youku
- YouTube

Am I required to provide password information?

No. Applicants are instructed to provide their usernames for these platforms—passwords are not requested or required. However, even without password information, immigration agencies likely will be able to review the full contents of your profiles.

Are there restrictions on what I can post on social media?

Many employers have social media policies in place. We recommend you confirm and comply with your employer's policies related to social media. Generally, it is advisable to refrain from posting the following:

- References to your employer's confidential company information; and/or
- Imply or create the impression that you are communicating the views of your employer, either on behalf of or as a representative of your employer.