Legal Update Article

Privacy Issues of U.S. Collection of Social Media Information from Visa Applicants

By Joseph J. Lazzarotti & Amy L. Peck

June 22, 2020

Meet the Authors

Joseph J. Lazzarotti
Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Amy L. Peck
Principal
402-391-1991
Amy.Peck@jacksonlewis.com

Related Services

Immigration
Privacy, Data and Cybersecurity

The Department of State (DOS) has been collecting (and maintaining) information on social media use from all visa applicants (immigrant and non-immigrant) since June 2019. The DOS's collection and maintenance of this information is the subject of a lawsuit.

Two common DOS forms, the DS-160 (Online Nonimmigrant Visa Application) and DS-260 (Application for Immigrant Visa and Alien Registration), require applicants to identify and provide user names for any of approximately 20 social media accounts (including the most popular ones) that they have used in preceding five years. The forms also ask, "Do you wish to provide information about your presence on any other websites or applications you have used within the last five years to create or share content (photos, videos, status updates, etc.)?" Although that question appears to be optional, a "No" answer appears to show up as a "No" to the question, not a "No" to the option — further complicating responses.

With this new information, the DOS, in real time, will have a detailed picture of the applicants' views and associations. Many questions have been raised about how this information will be used. These include:

- Will the DOS deny cases based upon perceptions of the applicant's views as expressed on social media?
- Is DOS looking for clues about possible criminal activities (such as substance abuse) or health-related issues (such as alcoholism)?
- Is the DOS looking for evidence of political organizing or affiliation with various political or social groups?
- How broadly is the DOS sharing this information with other government agencies and even foreign governments?

Despite claims of being part of the vetting process, concerns about privacy and misuse of information remain. While DOS could search the internet and social media channels for public information concerning visa applicants and use that information to validate applications or raise additional questions as appropriate, the information obtained from DS-160 and DS-260 Forms dramatically facilitate those efforts. A set of FAQs issued by DOS over a year ago attempted to address these concerns:

> **Is this just a way to profile individuals by their religion, political views, or race?**
>
> Consular officers cannot deny visas based on applicants' race, religion, ethnicity, national origin, political views, gender, or sexual orientation. The collection of social media identifiers is consistent with this. This information will be used for identity resolution and to determine whether the applicant is eligible for a U.S. visa under U.S. law. Visa ineligibilities are set forth in U.S. law. Consular officers will

not request user passwords and will not attempt to subvert any privacy controls applicants may have implemented on these platforms.

Could the collection of this information be considered an invasion of privacy?

No. The same safeguards and confidentiality provisions that already protect a visa applicant's personal information also apply to social media identifiers and all other newly collected information related to a visa application or adjudication. Consular officers will not request user passwords nor will they have any ability to modify privacy controls applicants may have implemented on these platforms. Maintaining robust screening standards for visa applicants is a dynamic practice that must adapt to emerging threats. We already request limited contact information, travel history, family member information, and previous addresses from all visa applicants. Collecting this additional information from visa applicants will strengthen our process for vetting applicants and confirming their identity. Consular officers would only use this information to determine the applicant's eligibility for a visa under existing U.S. law.

Information obtained from social media may not always be accurate, complete, or entirely in context, and minor, inadvertent mistakes on government forms could provide a basis to deny an application. Moreover, individuals are becoming more sensitive about their privacy. For example, under the California Consumer Privacy Act (CCPA), which became effective in January 2020, California residents have a right to know what categories of personal information covered organizations collect, why they collect it, the categories of sources they get it from, and the categories of third parties it is disclosed to. Visa applicants may have many of the same questions.

Digital privacy and government surveillance are growing concerns in America. A Pew Research Institute survey found that more than 80 percent of Americans feel a lack of control over the digital personal data that the government collects about them, and potential risks of collecting that data outweigh the benefits. The DOS's collection and maintenance of information on social media use from visa applicants calls into question fundamental U.S. privacy principles.

In December 2019, an organization of documentary filmmakers, along with Columbia University's Knight First Amendment Institute and the Brennan Centre for Justice, filed suit in federal court seeking an injunction and challenging this new "digital surveillance regime that enables the U.S. government to monitor visa applicants' constitutionally protected speech and association not just at the time they apply for visas, but even after they enter the United States." The organization relies on social media to share content, draw attention to human rights abuses, and facilitate partnerships and fundraising for social justice impact campaigns. The plaintiffs contend that the collection of this data chills First Amendment rights and causes applicants to engage in self-censorship by deleting content, avoiding posting, and simply not applying for visas to come to United States to engage in collaborations. They also contend that stripping applicants of anonymity by requiring the disclosure of pseudonyms may even put applicants in danger — if the information is shared with authoritarian governments. Recently, social media companies have filed amicus briefsin the case contending that the surrender of anonymity "violates the First Amendment rights to speak anonymously and associate privately."

Visa applicants may want to seek advice regarding their social media use. Failure to disclose or misrepresentation on the application forms could lead to serious consequences and is not an option. It is important to review social media content to determine whether admissibility issues might be raised.

Jackson Lewis attorneys are available to assist you in identifying possible issues and strategizing on how best to move forward.