Protecting Data While Traveling Internationally: An Employer's Guide for Foreign Nationals and Other Global-Traveling Workers

Insights
4.10.25

International travel may pose serious data security risks – especially for your foreign national workers carrying sensitive, proprietary, or regulated information. Travelers must be aware of potential border inspections, surveillance practices abroad, and export control regulations that may impact their devices and data. What does your organization need to know about these significant risks, and what can employers do to safeguard their information?

Quick Background on Border Searches

In countries like the United States, border agents can inspect electronic devices without a warrant or suspicion of wrongdoing. While the Fourth Amendment protects against unreasonable searches, this protection does not full apply to searches at the U.S. border.

Searches can range from viewing accessible content on an unlocked device to requesting passwords, accessing encrypted files, or copying data for forensic review. And it's not just foreign nationals subject to these searches. U.S. citizens and permanent residents are also subject to these inspections, even when entering lawfully. This is why professionals carrying confidential information should take extra precautions, as your company data may be accessed or copied – and your workers could be detained.

Other Data Security Risks

But it's not just border searches that can lead to loss of data. Once inside a country, travelers – especially foreign nationals – may face a range of digital security threats that go beyond airport inspections.

Surveillance Dangers

Network surveillance is common in many regions, particularly when using public Wi-Fi in hotels, airports, or cafes, where communications can be intercepted or monitored without the user's knowledge.

- In some countries, there are legal restrictions or outright bans on the use of encryption tools, making it more difficult for travelers to protect their data.

- Countries with higher risks for such activities include China, Russia, Iran, North Korea, and certain parts of the Middle East, where government surveillance is particularly aggressive.

Cybertheft

In addition to state-sponsored monitoring, cyber criminals often exploit these same environments, targeting unsecured connections to steal sensitive data, login credentials, or financial information. Travelers unaware of these risks may become easy targets for man-in-the-middle attacks or malware installations, especially when using outdated software or unsecured devices.

Export Control Considerations

Carrying certain data, software, or technologies abroad may trigger export control laws, especially in fields like defense, technology, and pharmaceuticals. Even encrypted files on a laptop can violate export laws if shared or accessed abroad. In the U.S., laws like ITAR and EAR impose serious penalties for violations.

Ethical and Legal Responsibilities

Professionals in law, research, journalism, and academia may be ethically or legally obligated to protect sensitive data. A New York State Bar ethics opinion, for example, concludes that attorneys must take "reasonable precautions" to avoid ethical breaches at borders. Third-party access of devices may also constitute a data breach that would require disclosure.

What Steps Can Your Organization Take?

Here are some recommended safeguards to help avoid a security breach or device access when your workers travel internationally:

- Instruct your workers to use VPNs or virtual desktops (if permitted).
- Prohibit them from using unsecured networks for sensitive communication.
- Require them to be wary of unknown USB devices or file transfers.
- Instruct workers to bring only essential devices and data when traveling internationally.
- Train them on maintaining strict control over their digital footprint while abroad.
- Use encrypted or "clean" loaner devices with minimal data.
- Require them to store confidential information in secure, institution-approved cloud platforms, not on devices.
- Ensure your compliance team has provided guidance on whether your data or software is export-controlled.
- Require your workers to use strong passwords and disable biometrics before crossing borders.

- Have your workers back up important data before departure.
- Require workers who travel abroad to disclose such travel with IT, legal, or compliance teams.
- Develop institutional data handling policies for international trips and train your workers on best practices.

Conclusion

In an era of digital mobility, data protection is essential. By preparing properly – through encryption, legal awareness, and secure data practices – foreign nationals can reduce their risk and travel with confidence. If you have any questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Immigration Practice Group, our FP Global Mobility team, or our Data Protection and Cybersecurity Team. We will provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.

Related People

David S. Jones
Regional Managing Partner
901.526.0431
Email

Service Focus

Immigration

Privacy and Cyber

International

Global Mobility