What Is the Privacy Shield?
The Privacy Shield is a government-backed voluntary program that creates a mechanism for companies to transfer personal data from the European Union to the United States, consistent with EU privacy laws. Companies that enroll in the program commit to a set of enforceable privacy protections designed to satisfy standards and safeguards established by EU privacy laws.

Who Uses the Privacy Shield?
The Privacy Shield is critical to a range of companies, including small businesses that serve customers in the EU and larger businesses with EU-based employees. Without the Privacy Shield, those businesses would need to undertake more challenging and costly measures to ensure they can send personal data from the EU to the US consistent with EU privacy laws.

As of October 2019, more than 5,000 companies from across the US are using the Privacy Shield. These businesses are contributing significantly to the nearly $1.1 trillion in US total trade in goods and services with the EU.

Companies that use the Privacy Shield include:

- **Small Businesses**: More than 70 percent of the more than 5,000 companies certified to the Privacy Shield program are small or medium-sized businesses. For example, small businesses that sell products or services to customers in the EU may rely on the Privacy Shield to send data about those customers to the US.

- **Consumer-Facing Companies**: Consumers rely on smartphones, tablets, and other connected devices that require service providers to move data throughout the world. For example, companies may need to transfer data across borders to let consumers watch streaming services, pay their bills online, access cloud-based services, or interact with customer support agents.

- **Companies Across a Range of Industries**: The Privacy Shield helps companies across industries transfer personal data to the US, including data about EU customers and EU employees. Companies in the automotive, finance, hospitality, logistics, health care, manufacturing and human resource management fields are certified to the Privacy Shield program.
Why Do We Need a Privacy Shield?

Businesses of all sizes—and all industries—must move data from one country to another. But EU law generally prohibits companies from transferring personal data in the EU to another country, unless that country provides “adequate” privacy protections. Companies that participate in the Privacy Shield commit to implementing a series of privacy safeguards, and can then rely on the Privacy Shield to send personal data from the EU to the US, consistent with EU law.

Why Is the Privacy Shield in Danger?

In recent months, European courts have heard two cases relating to the Privacy Shield. (BSA is participating as an intervenor in both cases.) The parties bringing those cases have challenged both the Privacy Shield and another method for transferring personal data outside the EU. The parties argue these methods for transferring data do not adequately protect the personal data of EU citizens. If the Privacy Shield is struck down, it would jeopardize the ability of companies participating in the program to send personal data from the EU to the US. Without the Privacy Shield, many of those companies may be unable to continue to provide services in the EU.

What Can Governments Do?

If Privacy Shield is invalidated, policymakers may need to act quickly to ensure that companies, including small businesses, can continue to send personal data from the EU to the US. Policymakers should be aware of the potential threat to transatlantic trade posed by the pending EU court case, in which a decision is expected in early 2020. Congress should be prepared to support efforts that ensure companies can continue to move data across borders.

How Does the Privacy Shield Work?

The Privacy Shield program is administered by the International Trade Administration within the Department of Commerce. Companies choose whether to join the voluntary program, but once a company publicly commits to comply with the Privacy Shield, that commitment is enforceable under US law by the Federal Trade Commission.

To join the Privacy Shield program, a company must:

1. Be subject to jurisdiction of the Federal Trade Commission or the Department of Transportation.
2. Publicly commit to the Privacy Shield Principles, a series of 23 principles that limit how companies can handle data received from the EU under the Privacy Shield. Companies must commit to these principles through a public-facing privacy policy.
3. Identify a recourse mechanism that individuals can use to investigate unresolved complaints, without cost.
4. Join the binding arbitration mechanism that can be used to determine if an organization has violated the Privacy Shield Principles.
5. Have a mechanism to verify the company complies with the Privacy Shield.
6. Designate an employee to handle questions about the Privacy Shield, as well as complaints and access requests.
7. Submit a self-certification to the Department of Commerce.

After joining the Privacy Shield, a company must maintain compliance, including annually re-certifying its compliance to the Department of Commerce.