
# Data Flows, Online Privacy, and Trade Policy

March 11, 2019

**Congressional Research Service**
https://crsreports.congress.gov
R45584

**CRS REPORT**
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R45584

March 11, 2019

**Rachel F. Fefer**
Analyst in International Trade and Finance

# Data Flows, Online Privacy, and Trade Policy

"Cross-border data flows" refers to the movement or transfer of information between computer servers across national borders. Such data flows enable people to transmit information for online communication, track global supply chains, share research, provide cross-border services, and support technological innovation.

Ensuring open cross-border data flows has been an objective of Congress in recent trade agreements and in broader U.S. international trade policy. The free flow of personal data, however, has raised security and privacy concerns. U.S. trade policy has traditionally sought to balance the need for cross-border data flows, which often include personal data, with online privacy and security. Some stakeholders, including some Members of Congress, believe that U.S. policy should better protect personal data privacy and security, and have introduced legislation to set a national policy. Other policymakers and analysts are concerned about increasing foreign barriers to U.S. digital trade, including data flows.

Recent incidents of private information being shared or exposed have heightened public awareness of the risks posed to personal data stored online. Consumers' personal online data is valued by organizations for a variety of reasons, such as analyzing marketing information and easing the efficiency of transactions. Concerns are likely to grow as the amount of online data organizations collect and the level of global data flows expand. As Congress assesses policy options, it may further explore the link between cross-border data flows, online privacy, and trade policy; the trade implications of a comprehensive data privacy policy; and the U.S. role in establishing best practices and binding trade rules that seek to balance public policy priorities.

There is no globally accepted standard or definition of data privacy in the online world, and there are no comprehensive binding multilateral rules specifically about cross-border data flows and privacy. Several international organizations, including the Organization for Economic Co-operation and Development (OECD), G-20, and Asia-Pacific Economic Cooperation (APEC) forum have sought to develop best practice guidelines or principles related to privacy and cross-border data flows, although none are legally binding. U.S. and other recent trade agreements are establishing new enforceable trade rules and disciplines.

Countries vary in their data policies and laws; some focus on limiting access to online information by restricting the flow of data beyond a country's borders, aiming to protect domestic interests (e.g., constituents' privacy). However, these policies can also act as protectionist measures. The EU and China, two top U.S. trading partners, have established prescriptive rules on cross-border data flows and personal data from different perspectives. The EU General Data Protection Regulation (GDPR) is driven by privacy concerns; China is focused on security. Their policies affect U.S. firms seeking to do business in those regions, as well as in other markets that emulate the EU and Chinese approaches. Unlike the EU or China, the United States does not broadly restrict cross-border data flows and has traditionally regulated privacy at a sectoral level to cover data, such as health records.

U.S. trade policy has sought to balance the goals of consumer privacy, security, and open commerce. The proposed United States-Mexico-Canada Agreement (USMCA) represents the Trump Administration's first attempt to include negotiated trade rules and disciplines on privacy, cross-border data flows, and security in a trade agreement. While the United States and other countries work to define their respective national privacy strategies, many stakeholders seek a more global approach that would allow interoperability between differing national regimes to facilitate and remove discriminatory trade barriers to cross-border data flows; this could offer an opportunity for the United States to lead the global conversation.

Although Congress has examined issues surrounding online privacy and has considered multiple bills, there is not yet consensus on a comprehensive U.S. online data privacy policy. Congress may weigh in as the Administration seeks to define U.S. policy on data privacy and engages in international negotiations on cross-border data flows.

# Contents



## Figures



## Contacts

# Overview

Cross-border data flows underlie today's globally connected world and are essential to conducting international trade and commerce. Data flows enable companies to transmit information for online communication, track global supply chains, share research, and provide cross-border services. One study estimates that digital commerce relying on data flows drives 22% of global economic output, and that global GDP will increase by another $2 trillion by 2020 due to advances in emerging technologies.[1] However, while cross-border data flows increase productivity and enable innovation, they also raise concerns around the security and privacy of the information being transmitted.

Cross-border data flows are central to trade and trade negotiations as organizations rely on the transmission of information to use cloud services, and to send non-personal corporate data as well as personal data to partners, subsidiaries, and customers. U.S. policymakers are considering various policy options to address online privacy, some of which could affect cross-border data flows. For example, new consumer rights to control their personal data may impact how companies can use such data. To enable international data flows and trade, the United States has aimed to eliminate trade barriers and establish enforceable international rules and best practices that allow policymakers to achieve public policy objectives, including promoting online security and privacy.

Building consensus for international rules and norms on data flows and privacy has become increasingly important as recent incidents have heightened the public's awareness of the risk of personal data stored online. For example, the 2018 Cambridge Analytica scandal drew attention because the firm reportedly acquired and used data on more than 87 million Facebook accounts in an effort to influence voters in the 2016 U.S. presidential election and the UK referendum on continued European Union (EU) membership ("Brexit").[2] In addition, security concerns have been raised about data breaches, such as those that exposed the personal data of half a million Google users or 500 million Marriot hotel customers.[3]

Organizations value consumers' personal online data for a variety of reasons. For example, companies may seek to facilitate business transactions, analyze marketing information, detect disease patterns from medical histories, discover fraudulent payments, improve proprietary algorithms, or develop competitive innovations. Some analysts compare data to oil or gold, but unlike those valuable substances, data can be reused, analyzed, shared, and combined with other information; it is not a scarce resource.

However, personal data is considered personal private property. Individuals often want to control who accesses their data and how it is used. Experts suggest that data may therefore be considered both a benefit and a liability that organizations hold. Data has value, but an organization takes on risk by collecting personal data; they become responsible for protecting users' privacy and not

[1] Mark Knickrehm, Bruno Berthon, and Paul Daugherty, "Digital Disruption: The Growth Multiplier," Accenture, January, 2016.

[2] Alvin Chang, "The Facebook and Cambridge Analytica scandal, explained with a simple diagram," *Vox*, May 2, 2018, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

[3] Gabriella Munoz, "Sen. Chuck Grassley hits Google with questions about security breach," *The Washington Times*, October 12, 2018, and Taylor Telford and Craig Timberg, "Marriott discloses massive data breach affecting up to 500 million guests," *The Washington Post*, November 30, 2018.

misusing the information. Data privacy concerns may become more urgent as the amount of online information organizations access and collect, and the level of global data flows, continue to expand.[4]

Countries vary in their policies and laws on these issues. The United States has traditionally supported open data flows and has regulated privacy at a sectoral level to cover data, such as health records, rather than create a comprehensive policy. U.S. trade policy has sought to balance the goals of consumer privacy, security, and open commerce, including eliminating trade barriers and opening markets. Other countries are developing data privacy policies that affect international trade as some governments or groups seek to limit data flows outside of an organization or across national borders for a number of reasons. Blocking international data flows may impede the ability of a firm to do business or of an individual to conduct a transaction, creating a form of trade protectionism. Research demonstrates not only the economic gains from digital trade and international data flows, but also the real economic costs of restrictions on such flows.[5]

For many policymakers, the crux of the issue is: How can governments protect individual privacy in the least trade-restrictive way possible? The question is similar to concerns raised about ensuring cybersecurity while allowing the free flow of data. In recent years, Congress has examined multiple issues related to cross-border data flows and online privacy.

In the 115th Congress, Congressional committees held hearings on these topics,[6] introduced multiple bills,[7] and conducted oversight over federal laws on related issues such as data breach notification.[8] Members are introducing new bills and holding hearings in the 116th Congress.[9] Congress may consider the proposed U.S.-Mexico-Canada Agreement (USMCA) and examine the digital trade chapter as an example of how to address the issues through trade agreements.

## Defining Online Privacy

In most circumstances, a consumer expects both privacy and security when conducting an online transaction. However, users' expectations and values may vary and there is no globally accepted standard or definition of data privacy in the online world. In addressing online privacy, Congress

[4] One source estimates 2.5 quintillion bytes of data are generated globally daily, https://www.iflscience.com/technology/how-much-data-does-the-world-generate-every-minute/.

[5] Aaditya Mattoo and Joshua Meltzer, "International Data Flows and Privacy," World Bank, p. 6, May 2018.

[6] For example, U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, *Oversight of the Federal Trade Commission*, 115th Cong., November 27, 2018; U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Digital Commerce and Consumer Protection, *21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies' Impact on U.S. Jobs*, 115th Cong., October 12, 2017; U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act*, 115th Cong., October 10, 2018; and U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Examining Safeguards for Consumer Data Privacy*, 115th Cong., September 26, 2018.

[7] See for example, H.R. 2520, S. 2728, S. 3744, and H.R. 5815.

[8] For more information on data breach notification laws, see CRS Legal Sidebar LSB10210, *What Legal Obligations do Internet Companies Have to Prevent and Respond to a Data Breach?*, by Chris D. Linebaugh.

[9] For example, S. 142 and S. 189; U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce, *Protecting Consumer Privacy in the Era of Big Data*, 116th Cong., February 26, 2019; U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Subcommittee on Commerce, Science, and Transportation, *Policy Principles for a Federal Data Privacy Framework in the United States*, committee print, 116th Cong., February 27, 2019; U.S. Congress, Senate Committee on the Judiciary, *GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation*, 116th Cong., March 12, 2019.

may need to define personal data and differentiate between sensitive and non-sensitive personal data. In general, data privacy can be defined by an individual's ability to prevent access to personally identifiable information (PII).

According to the U.S. Office of Management and Budget (OMB) guidance to federal agencies, PII refers to:

> information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.[10]

Since electronic data can be readily shared and combined, some data not traditionally considered PII may have become more sensitive. For example, the OMB definition does not specifically mention data on location tracking, purchase history, or preferences, but these digital data points can be tracked by a device such as a mobile phone or laptop that an individual carries or logs into. The EU definition of PII attempts to capture the breadth of data available in the online world:

> "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[11]

Policymakers may consider differentiating between sensitive and non-sensitive personal data. For example, sensitive personal data could include ethnic origin, political or religious affiliation, biometric data, health data, sexual orientation, precise geolocation data, etc.

## Cross-Border Data Flows and Online Privacy

"Cross-border data flows" refers to the movement or transfer of information between computer servers across national borders. Cross-border data flows are part of, and integral to, digital trade and facilitate the movement of goods, services, people, and finance. A 2017 analysis estimated that global flows of goods, services, finance, and people increased world gross domestic product (GDP) by at least 10% in the past decade, adding $8 trillion between 2005 and 2015.[12] Effective and sustainable digital trade relies on data flows that permit commerce and communication but that also ensure privacy and security, protect intellectual property, and build trust and confidence. Impeding cross-border data flows, including through some privacy regulations, may decrease efficiency and reduce other benefits of digital trade, resulting in the fracturing, or so-called balkanization, of the internet.[13]

In addressing online privacy, some policymakers focus on limiting access to online information by restricting the flow of data beyond a country's borders. Such limits may also act as protectionist measures. Online privacy policies may create barriers to digital trade, or damage trust in the underlying digital economy. For example, measures to limit cross-border data flows could:

---

[10] Office of Management and Budget, OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 2017. This definition is based on OMB Circular No. A-130, *Managing Information as a Strategic Resource*, July 28, 2016.

[11] European Union General Data Protection Regulation Article 4.

[12] Jacques Bughin and Susan Lund, "The ascendancy of international data flows," McKinsey Global Institute, January 9, 2017.

[13] A. Michael Spence, "Preventing the Balkanization of the Internet," The Council on Foreign Relations, March 18, 2018.

- block companies from using cloud computing to aggregate and analyze global data, or from gaining economies of scale,
- constrain e-commerce by limiting international online payments,
- hinder global supply chains seeking to use blockchain to track products, manage supply chains, customs documentation, or electronic payments,[14]
- impede the trading of crypto-currency, or
- limit the use of advanced technology like artificial intelligence.[15]

According to the World Trade Organization (WTO), one of the most significant overall impacts of the growth of digital technologies is in transforming international trade. Technology can lower the costs of trade, change the types of goods and services that are traded, and may even change the factors defining a country's comparative advantage.[20] The extent of the impact of digital technologies on trade, however, depends in large part on open cross-border data flows.

**Business and Cross-Border Data Flows**

- Data flows (terabits per second) grew by a factor of 45 from 2005 to 2016.[16]
- More than 50% of businesses globally rely on data flows for cloud computing.[17]
- Skype, a voice-over-internet-protocol (VoIP) service that accounted for 30% of global communication in 2016, depends on international data flows.[18]
- Data localization rules impeding data flows are the #1 digital trade barrier cited by U.S. firms.[19]

One study of U.S. companies found that data localization rules (i.e., requiring organizations to store data on local servers) were the most-cited digital trade barrier.[21] Some governments advocate privacy or security policies that require data localization and limit cross-border data flows. However, many industry stakeholders argue that blocking cross-border data flows and storing data domestically does not make such data more secure or private.[22]

[14] Blockchain is a decentralized, distributed record or ledger of transactions in which the transactions are stored in a permanent using cryptography. For more information on blockchain and international trade, see CRS In Focus IF10810, *Blockchain and International Trade*, by Rachel F. Fefer.

[15] Artificial intelligence can generally be thought of as computerized systems that work and react in ways commonly thought to require intelligence, such as solving complex problems in real-world situations. For more information, see CRS In Focus IF10608, *Overview of Artificial Intelligence*, by Laurie A. Harris.

[16] Jacques Bughin and Susan Lund, "The ascendancy of international data flows," McKinsey Global Institute, January 9, 2017.

[17] U.S. International Trade Commission, *Global Digital Trade 1:Market Opportunities and Key Foreign Trade Restrictions*, Investigation Number: 332-561, August 2017.

[18] Ibid.

[19] Ibid.

[20] WTO, "World Trade Report 2018: The future of world trade," https://www.wto.org/english/res_e/publications_e/wtr18_e.htm.

[21] U.S. International Trade Commission, *Global Digital Trade 1:Market Opportunities and Key Foreign Trade Restrictions*, Investigation Number: 332-561, August 2017.

[22] Lindsay Bednar, "Locking Data Behind National Borders Is Unjustified and Causes Self-Inflicted Wounds, ITIF Testifies Before U.S. International Trade Commission," Information Technology and Innovation Foundation (ITIF), April 4, 2017.

## Balancing Policy Objectives

Many experts argue that policymakers should limit cross-border data flows in the least trade-restrictive manner possible and also ensure security and privacy. These objectives are not easily reconciled. Moreover, although an overlap exists between data protection and privacy, the two are not equivalent.

Cybersecurity measures are essential to protect data (e.g., against intrusions or theft by hackers). However, they may not be sufficient to protect privacy. For example, if an organization shares user data with a third party, it may be doing so securely, but not in a way that protects users' privacy or aligns with consumer expectations. Similarly, breach notification requirements are not the same as proactive privacy protection measures.[23] At the same time, policies that protect a consumer's privacy can align with security policies. Laws can limit law enforcement's access to information except in certain circumstances. Keeping user information anonymous may enable firms to analyze data while protecting individuals' identities.

Some see an inherent conflict between online security, privacy, and trade; others believe that policies protecting all three can be coherent and consistent.[24] The U.S. government has traditionally sought to balance these objectives. Some stakeholders note, however, that current U.S. policy has been inadequate in protecting online privacy and that change is needed. In some cases in the past, Congress has acted to address privacy concerns in particular sectors; for example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 led to health privacy standards regulations.[25] The Trump Administration has begun an effort to devise an overarching data privacy policy (see "Defining the U. S. Approach") and many Members of Congress are also considering possible approaches.

# Multilateral Rules

There are no comprehensive multilateral rules specifically about privacy or cross-border data flows. However, the United States and other countries have begun to address these issues in negotiating new and updated trade agreements, and through international economic forums and organizations such as the Asia-Pacific Economic Cooperation (APEC) and Organization for Economic Co-operation and Development (OECD).

## WTO General Agreement on Trade in Services

The World Trade Organization (WTO) General Agreement on Trade in Services (GATS) entered into force in January 1995, predating the current reach of the internet and the explosive growth of global data flows.[26] Many digital products and services that did not exist when the agreements were negotiated are not covered. On the other hand, privacy is explicitly addressed within GATS as an exception to allow countries to take measures that do not conform with the agreement in order to protect "the privacy of individuals in relation to the processing and dissemination of

[23] For more information on data breach notification laws, see CRS Legal Sidebar LSB10210, *What Legal Obligations do Internet Companies Have to Prevent and Respond to a Data Breach?*, by Chris D. Linebaugh.

[24] Multiple witness testimonies during U.S. International Trade Commission hearing on "Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions," April 4, 2017.

[25] For more information on HIPAA, please see CRS Report R43991, *HIPAA Privacy, Security, Enforcement, and Breach Notification Standards*, by C. Stephen Redhead.

[26] The full text of the WTO GATS is available at: https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm.

personal data and the protection of confidentiality of individual records and accounts," as long as those measures are not arbitrary or a disguised trade restriction.[27]

Efforts to update the multilateral agreement and discussions for new digital trade rules under the WTO Electronic Commerce Work Program stalled in 2017.[28] Given the lack of progress on multilateral rules, some have suggested that the WTO should identify best practices or guidelines for digital trade rules that could lay the foundation for a future multilateral WTO agreement.

## WTO Plurilateral Effort

In December 2017, a group of more than 70 WTO members, including the United States, agreed to "initiate exploratory work together toward future WTO negotiations on trade-related aspects of electronic commerce."[29] Overall U.S. objectives include allowing the free flow of information for international trade and cross-border data flows, "subject to reasonable safeguards like the protection of consumer data when it is exported," but do not specifically address privacy.[30]

The group formally launched the e-commerce initiative in January 2019.[31] The official joint statement lists the United States and EU as participants, and also several developing countries such as China and Brazil. India stated it will not join, preferring to maintain its flexibility to favor domestic firms, limit foreign market access, and raise revenue in the future.[32]

The statement did not define the scope of any potential agreement. After the meeting, the EU noted data localization measures among the potential new rules to be discussed when negotiations officially launch in March 2019.[33] The U.S. Trade Representative's (USTR) statement emphasized the need for a high-standard agreement that includes enforceable obligations.[34] Although some experts note that harmonization or mutual recognition is unlikely given divergent legal systems, privacy regimes, and norms of the parties, a common system of rules to allow for cross-border data flows while ensuring privacy protection is reportedly under discussion.[35]

# International Guidelines and Best Practices

Personal privacy has received increasing focus with the growth of digital trade encouraging global cooperation. The United States has contributed to developing international guidelines or principles related to privacy and cross-border data flows, although none are legally binding.

[27] WTO GATS Article XIV.

[28] For more information on the WTO, see CRS Report R45417, *World Trade Organization: Overview and Future Direction*, coordinated by Cathleen D. Cimino-Isaacs; WTO General Council, "Work Programme on Electronic Commerce Report by the Chairman," WT/GC/W/739, December 1, 2017.

[29] WTO, "Joint Statement on Electronic Commerce," December 13, 2017, https://ustr.gov/sites/default/files/files/Press/Releases/Joint%20Statement%20on%20Electronic%20Commerce.pdf.

[30] WTO, "Joint Statement on Electronic Commerce Initiative Communication from the United States," JOB/GC/178, April 12, 2018.

[31] WTO Joint Statement on Electronic Commerce, WT/L/1056, January 25, 2019.

[32] Subhayan Chakraborty, "India refuses to join e-commerce talks at WTO, says rules to hurt country," *The Business Standard*, February 25, 2019.

[33] European Commission, "75 countries launch WTO talks on e-commerce," Press Release Database, January 25, 2019.

[34] USTR, "USTR Robert Lighthizer on the Joint Statement on Electronic Commerce," January 25, 2019, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2019/january/ustr-robert-lighthizer-joint.

[35] "Japan, US and EU to establish data transfer rules," *Nikkei Asian Review*, December 18, 2018.

## OECD

The OECD *1980 Privacy Guidelines* established the first international set of privacy principles emphasizing data protection as a condition for the free flow of personal data across borders.[36] These OECD guidelines were intended to assist countries with drawing up national data privacy policies.

The guidelines were updated in 2013, focusing on national level implementation based on a risk management approach and improving interoperability between national privacy strategies.[37] The updated guidelines identify specific principles for countries to take into account in establishing national policies. The guidelines are to be reviewed and updated again in 2019.

**OECD Privacy Guidelines: Principles for Personal Data Collection**

- Collection should be
  - lawful, fair, and with the consent of the individual;
  - accurate, complete, up-to-date; and
  - limited to fulfill the specified purpose.
- Data should
  - not be disclosed or made available without consent or by legal authority;
  - be protected by security safeguards; and
  - available for establishing existence, nature, and purpose.
- Individuals should have the right to access personal data collected and challenge data to correct, amend, or delete.
- Data controller should be accountable for compliance.

## G-20

Building on the OECD principles and prior G-20 work, the 2018 G-20 Digital Economy Ministerial Declaration identified principles to "facilitate an inclusive and whole-of-government approach to the use of information and communication technology (ICT) and assist governments in reshaping their capacities and strategies, while respecting the applicable frameworks of different countries, including with regards to privacy and data protection."[38]

Japan is to host the 2019 G-20 and plans to focus on data governance, offering a forum to address potential global standards on privacy and cross-border data flows.

## APEC

APEC is a regional forum for economic cooperation whose initiatives on privacy and cross-border data flows have influenced members' domestic policies. APEC's 21 members, including the United States, agreed to the *2005 APEC Privacy Framework*, based on the OECD guidelines. The framework identifies a set of principles and implementation guidelines to provide members with a flexible approach to regulate privacy at a national level.[39] Once the OECD publishes

[36] OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 1980, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[37] OECD, "Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 2013, http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

[38] G-20 Digital Economy Ministerial Declaration, "G-20 Digital Economy," August 24, 2018.

[39] APEC CTI Sub-Fora & Industry Dialogues Groups, Electronic Commerce Steering Group (ECSG), "APEC Privacy Framework," APEC#205-SO-01.2, December 2005, https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework.

updated guidelines in 2019, APEC members may revise the framework and principles to reflect the updated guidelines.

**APEC Privacy Framework Principles**

- Design privacy protection measures to prevent misuse of personal information
- Provide clear notice about personal data collection
- Lawfully collect only relevant information as needed
- Use personal information only for specific purposes
- Give individuals choice for data collection
- Update, correct personal data collected
- Establish security safeguards to protect data
- Allow individuals access and ability to correct data
- Ensure compliance and accountability of information controller

## APEC CBPR

The APEC Cross-Border Privacy Rules (CBPR), endorsed by APEC Leaders in 2011, is a privacy code of conduct, based on the framework. The CBPR system establishes a set of principles for governments and businesses to follow to protect personal data and allow for cross-border data flows between CBPR members.[40] They aim to balance information privacy with business needs and commercial interests, and facilitate digital trade to spur economic growth in the region.

Rather than creating a new set of international regulations, the APEC framework and CBPR system identify best practices that each APEC member can tailor to its domestic legal system and allows for interoperability between countries. The scope and implementation mechanisms under CBPR can vary according to each member country's laws and regulations, providing flexibility for governments to design national privacy approaches. To become a member of the CBPR, a government must

1. Be a member of APEC;
2. Establish a regulator with authority to sign the Cross-Border Privacy Enforcement Arrangement (CPEA);
3. Map national laws to the published APEC guidelines which set baseline standards; and
4. Establish an accountability agent empowered to audit and review a company's practices, and enforce privacy rules and laws.

If a government joins the CBPR system, every domestic organization is not required to also join; however, becoming a member of CBPR may benefit an organization engaged in international trade by indicating to customers and partners that the organization values and protects data privacy. With certified enrollment in CBPR, organizations can transfer personal information between participating economies (e.g., Mexico to Singapore) and be assured of compliance with the legal regimes in both places. To become a CBPR member, an individual organization must develop and implement data privacy policies consistent with the APEC Privacy Framework and complete a questionnaire. The third party accountability agent is responsible for assessing an organization's application, ongoing monitoring of compliance, investigating any complaints, and taking enforcement actions as necessary.[41] Domestic enforcement authorities in each member country serve as a backstop for dispute resolution if an accountability agent cannot resolve a particular issue. All CBPR member governments must join the CPEA to ensure cooperation and collaboration between the designated national enforcement authorities.

[40] http://cbprs.org/.

[41] More information on APEC CBPR accountability agents is available at: http://cbprs.org/accountability-agents/.

In the United States, the Federal Trade Commission (FTC) is the regulator and enforcement authority. TrustArc is the only accountability agent, but many expect the U.S. Department of Commerce to recognize additional agents soon. As of this writing, TrustArc lists about 20 U.S. firms that are APEC CBPR certified.[42]

### Expanding CBPR Beyond APEC

The CBPR grows in significance as the number of participating economies and organizations increases. The U.S. ambassador to APEC aims to have "as many APEC economies as possible as soon as possible to join the system."[43] Currently, the United States, Japan, Mexico, Canada, South Korea, Singapore, Taiwan, and Australia are CBPR members; the Philippines is in the process of joining. Russia, on the other hand, stated it has no plans to join. Although APEC initiatives are regionally focused, they can provide a basis to scale up to larger global efforts because they reflect economies at different stages of development and include industry participation. Due to its voluntary nature, APEC has served as a testbed for identifying best practices, standards, and principles and for creating frameworks that can lead to binding commitments in plurilateral or larger multilateral agreements (see "Data Flows and Privacy in U.S. Trade Agreements").

Expanding CBPR beyond APEC could represent the next step toward consistent international rules and disciplines on data flows and privacy.

## Foreign Government Policies

Countries vary in their privacy policies and laws, reflecting differing priorities, cultures, and legal structures. According to one index, China is the most restrictive digital trade country among 64 countries surveyed, followed by Russia, India, Indonesia, and Vietnam (see **Figure 1**).[44] The United States ranks 22 in the index, less restrictive than Brazil or France but more restrictive than Canada or Australia.[45] The relatively high U.S. score largely reflects financial sector restrictions.

Within the composite index, data policies include measures for security, privacy, or other justifications and falls within the "restrictions on data" category. Looking specifically at the 64 countries' data policies, Russia is the most restrictive country, followed by Turkey and China.[46] Russia's policies include data localization, retention, and transfer requirements, among others. Turkey's comprehensive Data Protection Law also establishes requirements in these areas.[47] In contrast, the United States ranks 50 for data policy restrictions.

Two of the top U.S. trading partners (the EU and China) have established their data policies from different perspectives. The EU's policies are driven by privacy concerns; China's policies are based on security justifications. Both are setting examples that other countries, especially those with (or seeking) closer trading ties to China or the EU, are emulating; thus, these policies have affected U.S. firms seeking to do business in those other countries as well.

[42] See https://www.trustarc.com/consumer-resources/trusted-directory/#list.

[43] "U.S. recruiting countries to join APEC privacy system," *World Trade Online*, February 7, 2019.

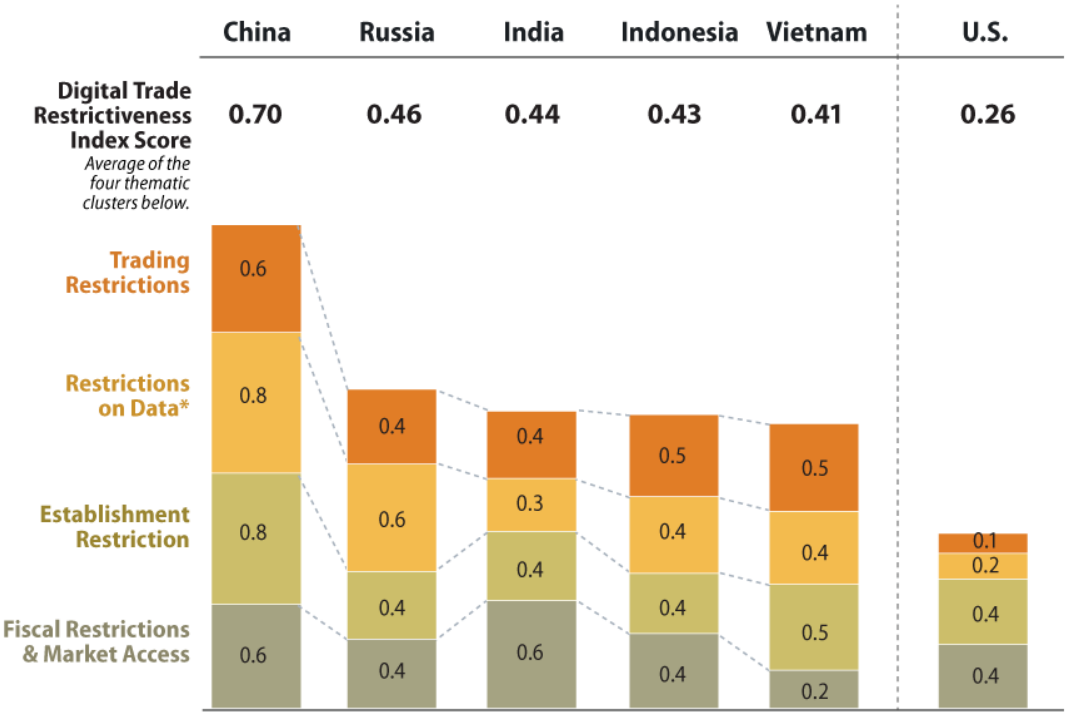
[44] ECIPE, "DTRI Trade Restrictiveness Index," April 2018, https://ecipe.org/dte/dte-report/.

[45] The index ranks individual countries and does not rank the EU as a single unit. The EU is composed of shared as well as non-shared competences among its member states; some measures in the index belong to individual EU member countries while others (such as data privacy regulations) are set at the EU level.

[46] Ibid, p.54.

[47] Turkish Personal Data Protection Law no. 6698 entered into force on April 7, 2016.

**Figure 1. Digital Trade Restrictiveness Index**




**Source:** ECIPE, Digital Trade Restrictiveness Index, April 2018.

**Notes:** *Includes data policies. All index scores reflect rounding.

# EU: Privacy First

## U.S.-EU Privacy Shield

The EU considers the privacy of communications and the protection of personal data to be fundamental human rights, which are codified in EU law.[48] Differences between the United States and EU in their approaches to data protection and data privacy laws, have long been sticking points in U.S.-EU economic and security relations. The EU and United States negotiated the U.S.-EU Privacy Shield to allow for the transatlantic transfer of personal data by certified organizations. The bilateral agreement established a voluntary program with commitments and obligations for companies, limitations on law enforcement access, and transparency requirements. U.S. companies that participate in the program must still comply with all of the obligations under EU law (see below) if they process personal data of EU persons. The Privacy Shield is overseen and enforced by EU federal and U.S. agencies, including the Department of Commerce and the FTC, and is reviewed by both parties annually.

[48] EU Charter of Fundamental Rights Title II Freedoms, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en.

## EU GDPR

The EU's General Data Protection Regulation (GDPR), effective May 2018, establishes rules for EU members, with extraterritorial implications.[49] The GDPR is a comprehensive privacy regime that builds on previous EU data protection rules. It grants new rights to individuals to control personal data and creates specific new data protection requirements.

The GDPR applies to (1) all businesses and organizations with an EU establishment that process (i.e., perform operations on) personal data of individuals in the EU, regardless of where the actual processing of the data takes place; and (2) entities outside the EU that offer goods or services (for payment or for free) to individuals in the EU or monitor the behavior of individuals in the EU. While the GDPR is directly applicable at the EU member state level, individual countries are responsible for establishing some national-level rules and policies as well as enforcement authorities, and some are still in the process of doing so. As a result, some U.S. stakeholders have voiced concerns about a lack of clarity and inadequate country compliance guidelines.

**EU's GDPR New Individual Rights:**

- Receive clear and understandable information about who is processing one's personal data and why.
- Consent affirmatively to any data processing.
- Access any personal data collected.
- Rectify inaccurate personal data.
- Erase one's personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data (the "right to be forgotten").
- Restrict or object to certain processing of one's data.
- Be notified without "undue delay" of a data breach if there is a high risk of harm to the data subject.
- Require the transmission of one's data to another controller (data portability).

Many U.S. firms doing business in the EU have made and are making changes to comply with the GDPR, such as revising and clarifying user terms of agreement and asking for explicit consent. For some U.S. companies, it may be easier and cheaper to apply GDPR protections to all users worldwide rather than to maintain different policies for different users. Large firms may have the resources to hire consultants and lawyers to guide implementation and compliance; it may be harder and costlier for small and mid-sized enterprises to comply, possibly deterring them from entering the EU market and creating a de facto trade barrier.

Since the GDPR went into effect on May 25, 2018, some U.S. businesses, including some newspaper websites and digital advertising firms, have opted to exit the EU market given the complexities of complying with the GDPR and the threat of potential enforcement actions.[50] European Data Protection Authorities (DPAs) have received a range of GDPR complaints and initiated several GDPR enforcement actions in the Fall of 2018. In January 2019, the French DPA issued the largest penalty to date for a data privacy breach. The agency imposed a €50 million (approximately $57 million) fine on Google for the "lack of transparency" regarding how the search engine processes user data.[51] Analysts contend that the high fine may set a benchmark and signal for future enforcement, raising concerns among some firms doing business in the EU.[52]

[49] The full text of the GDPR is available at https://gdpr-info.eu/. Also see CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick.

[50] "Websites not available in the European Union after GDPR," VerifiedJoseph.com, July 11, 2018, updated November 16, 2018, https://data.verifiedjoseph.com/dataset/websites-notavailable-eu-gdpr.

[51] Laura Kayali, "France hits Google with €50 million fine for GDPR violation," *Politico Pro*, January 21, 2019.

[52] Denis Charlet, "Big Google Privacy Fine May Set Bar for EU Privacy Penalties," *Bloomberg Law*, January 24, 2019.

## Exporting Personal Data under EU GDPR

Under the GDPR, a few options exist to transfer personal data in or out of the EU and ensure that privacy is maintained.

1. An organization may use specific Binding Corporate Rules (BCRs) or Model Contracts approved by the EU;
2. An organization may comply with domestic privacy regimes of a country that has obtained a mutual adequacy decision from the EU, which means that the EU has deemed that a country's laws and regulations provide an adequate level of data protection; currently, fewer than 15 jurisdictions are deemed adequate by the EU[53]; or
3. A U.S.-based organization may enroll in the bilateral U.S.-EU Privacy Shield program for transatlantic transfer of personal data.

The GDPR legal text seems to envision a fourth way, such as a certification scheme to transfer data, that the EU has yet to elaborate. A certification option(s) could create a less burdensome means of compliance for U.S. and other non-EU organizations to transfer personal data to or from the EU in the future. This could be an opportunity for the United States to work with the EU on creating a common system, perhaps even setting a global standard.

## Expanding GDPR Beyond the EU

Some experts contend that the GDPR may effectively set new global data privacy standards, since many companies and organizations are striving for GDPR compliance to avoid being shut out of the EU market, fined or otherwise penalized, or in case other countries introduce rules that imitate the GDPR.[54]

The EU is actively promoting the GDPR and some countries, such as Argentina, are imitating all or parts of the GDPR in their own privacy regulatory and legislative efforts or as part of broader trade negotiations with the EU.[55] In general, the EU does not include cross-border data flows or privacy in free trade agreements. However, alongside trade negotiations with Japan, the EU and Japan agreed to recognize each other's data protection systems as "equivalent," allowing for the free flow of data between the EU and Japan and serving as a first step in adopting an adequacy decision.[56] Under the agreement, Japan committed to implementing additional measures to address the handling of the personal data of EU persons on top of Japan's own privacy regime.[57]

[53] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

[54] For example, see Anick, Jesdanun, "Microsoft pledges to extend EU data rights worldwide," May 21, 2018.

[55] Pablo Palazzi, "New draft of Argentine data protection law open for comment," IAPP Privacy Tracker, February 17, 2017, and Diego Fernandez, "Argentina's new Bill on Personal Data Protection," IAPP Privacy Tracker, October 2, 2018.

[56] European Commission, "The European Union and Japan agreed to create the world's largest area of safe data flows," Press Release Database, July 17, 2018.

[57] European Commission, "European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows," Press Release Database, January 23, 2019.

## China: Security First

China's trade and internet policies reflect state direction and industrial policy, limiting the free flow of information and individual privacy. For example, the requirement for all internet traffic to pass through a national firewall can impede the cross-border transmission of data.[58] China's 2015 counterterrorism law requires telecommunications operators and internet service providers to provide assistance to the government, which could include sharing individuals' data. Citing national security concerns, China's Internet Sovereignty policies, Cybersecurity Law, and Personal Information Security Specification impose strict requirements on companies, such as storing data domestically; limiting the ability to access, use, or transfer data internationally; and mandating security assessments that provide Chinese authorities access to proprietary information.

In 2014, China announced a new social credit system, a centralized big-data-enabled system for monitoring and shaping businesses' and citizens' behavior that serves as a self-enforcing regulatory mechanism. According to the government, China aims to make individuals more "sincere" and "trustworthy," while obtaining reliable data on the creditworthiness of businesses and individuals. An individual's score would determine the level of government services and opportunities he or she could receive.[59]

China seeks to have all its citizens subject to the social credit system by 2020, forcing some U.S. businesses who do business in China, such as airlines, to participate.[60] As of 2018, multiple government agencies and financial institutions contribute data to the platform. Pilot projects are underway in some provinces to apply various rewards and punishments in response to data collected. The lack of control an individual may have and the exposure of what some consider private data is controversial among observers in and out of China.

Some countries, such as Vietnam, are following China's approach in creating cybersecurity policies that limit data flows and require local data storage and possible access by government authorities.[61] Some U.S. firms and other multinational companies are considering exiting the Vietnamese market rather than complying, while some analysts suggest that Vietnam's law may not be in compliance with its recent commitments in trade agreements (see below).[62] India has also cited security as the rationale for its draft Personal Data Protection Bill, which would establish broad data localization requirements and limit cross-border transfer of some data.[63] Unlike the EU, these countries do not specify mechanisms to allow for cross-border data flows. U.S. officials have raised concerns with both Vietnam's and India's localization requirements.[64]

[58] USTR, "2018 USTR Report to Congress on China's WTO Compliance," February 2019, p. 156.

[59] Kelsey Munro, "China's social credit system 'could interfere in other nations' sovereignty'," *The Guardian,* June 27, 2018.

[60] Jack Karsten and Darrell M. West, "China's social credit system spreads to more daily transactions," Brookings, June 18, 2018.

[61] Yee Chung Seck and Thanh Son Dang, "Vietnam National Assembly Passes the Law on Cybersecurity," Global Compliance News, July 2, 2018.

[62] Nigel Cory, "Vietnam's cybersecurity law threatens free trade," *Nikkei Asian Review*, August 15, 2018.

[63] INDUSLaw, "India: The Debate – Data Localization And Its Efficacy," September 17, 2018, mondaq.com.

[64] U.S. Trade Representative, *2018 National Trade Estimate Report on Foreign Trade Barriers*, 2018.

# Defining the U. S. Approach

The EU's emphasis on privacy protection and China's focus on national security (and the countries that emulate their policies) have led these countries to create data-focused policies that restrict international trade and commerce. The United States has traditionally sought a balanced approach between trade, privacy, and security.

U.S. data flow policy priorities are articulated in USTR's Digital 2 Dozen report, first developed under the Obama Administration,[65] and the White House's 2017 National Security Strategy.[66] Both Administrations emphasize the need for protection of privacy, the free flow of data across borders, and an interoperable internet. These documents establish the U.S. position that the free flow of data is not inconsistent with privacy protection. Recent free trade agreements translate the U.S. position into binding international commitments.

The United States has taken a data-specific approach to regulating data privacy, with laws protecting specific information, such as healthcare or financial data. The FTC enforces consumer protection laws and requires that consumers be notified of and consent to how their data will be used, but the FTC does not have the mandate or resources to enforce broad online privacy protections. There is growing interest among some Members of Congress and in the Administration for a more holistic U.S. data privacy policy.

## Data Flows and Privacy in U.S. Trade Agreements

The United States has played an important role in international discussions on privacy and data flows, such as in the OECD, G-20, and APEC, and has included provisions on these subjects in recent free trade agreements.

Congress noted the importance of digital trade and the internet as a trading platform in setting the current U.S. trade negotiating objectives in the June 2015 Trade Promotion Authority (TPA) legislation (P.L. 114-26). TPA includes a specific principal U.S. trade negotiating objective on "digital trade in goods and services and cross-border data flows." According to TPA, a trade agreement should ensure that governments "refrain from implementing trade-related measures that impede digital trade in goods and services, restrict cross-border data flows, or require local storage or processing of data."[67] However, TPA also recognizes that sometimes measures are necessary to achieve legitimate policy objectives and aims for such regulations to be the least trade-restrictive, nondiscriminatory, and transparent.

**Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP/TPP-11).** The CPTPP is a recently-concluded trade agreement between 11 Asia-Pacific countries.[68] The CPTPP is based on the proposed Trans-Pacific Partnership (TPP) agreement negotiated by the Obama Administration and from which President Trump withdrew the United States in January

[65] https://ustr.gov/sites/default/files/Digital-2-Dozen-Updated.pdf.

[66] https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

[67] P.L. 114-26, Title I (b)(6)(C).

[68] The CPTPP includes Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam. For more information on the digital trade provisions contained in the proposed TPP, see CRS In Focus IF10390, *TPP: Digital Trade Provisions*, by Rachel F. Fefer.

2017. The Electronic Commerce chapter in TPP, left unchanged in CPTPP, contains the strongest binding trade agreement commitments on digital trade in force globally. [69]

CPTPP includes provisions on cross-border data flows and personal information protection. The text specifically states that the parties "shall allow the cross-border transfer of information." [70] The agreement allows restrictive measures for legitimate public policy purposes if they are not discriminatory or disguised trade barriers. The agreement also prohibits localization requirements for computing facilities, with similar exceptions.

On privacy, the CPTPP requires parties to have a legal framework in place to protect personal information and to have consumer protection laws that cover online commerce. It encourages interoperability between data privacy regimes and encourages cooperation between consumer protection authorities.

**United States-Mexico-Canada Agreement (USMCA).** The released text for the proposed USMCA aims to revise and update the trilateral North American Free Trade Agreement (NAFTA), and illustrates the Trump Administration's approach.

The USMCA Chapter 19 on Digital Trade includes articles on consumer protection, personal information protection, cross-border transfer of information by electronic means, and cybersecurity, among other topics.[71] Building on the TPP, the agreement seeks to balance the legitimate objectives by requiring parties to:

- Have a legal framework to protect personal information.
- Have consumer protection laws for online commercial activities.
- Not prohibit or restrict cross-border transfer of information.

**USMCA Key Principles for Personal Information Protection**

- Limitation on collection
- Choice
- Data quality
- Purpose specification
- Use limitation
- Security safeguard
- Transparency
- Individual participation
- Accountability

While the agreement does not prescribe specific rules or measures that a party must take to protect privacy, it goes further than the TPP (or CPTPP) provisions and provides guidance to inform a country's privacy regime. In particular, the USMCA explicitly refers to the APEC Privacy Framework and OECD Guidelines as relevant and identifies key principles.

In general, the proposed USMCA requires that parties not restrict cross-border data flows. Governments are allowed to do so to achieve a legitimate public policy objective (e.g., privacy, national security), provided the measure is not arbitrary, discriminatory, a disguised trade barrier, or greater than necessary to achieve the particular objective. In this way, the parties seek to balance the free flow of data for commerce and communication with protecting privacy and security. The agreement specifically states that the parties may take different legal approaches to protect personal data and also

[69] CPTPP Chapter 14, available at https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf.

[70] CPTPP Chapter 14 Article 14.11.

[71] United States-Mexico-Canada Agreement, Chapter 19 as announced by the U.S. Trade Representative, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/19%20Digital%20Trade.pdf.

recognizes APEC CBPR as a "valid mechanism to facilitate cross-border information transfer while protecting personal information."[72]

The agreement aims to increase cooperation between the United States, Mexico, and Canada on a number of digital trade issues, including exchanging information on personal information protection and enforcement experiences; strengthening collaboration on cybersecurity issues; and promoting the APEC CBPR and global interoperability of national privacy regimes. The governments also commit to encourage private sector self-regulation models and promote cooperation to enforce privacy laws. While the agreement is only between three parties, the provisions are written broadly to encompass global efforts. Some stakeholders look at USMCA as the basis for potential future trade agreements (such as with the UK).[73] Cross-border data flows will likely be a key issue in future U.S.-EU trade negotiations.

## U.S. Federal Data Privacy Policy Efforts

The United States has articulated a clear position on data privacy in trade agreements; however, there is no single U.S. data privacy policy. Nevertheless, the Trump Administration is seeking to define an overarching U.S. policy on data privacy.[74] The Trump Administration's ongoing three-track process is being managed by the Department of Commerce (Commerce) in consultation with the White House. Different bureaus in Commerce are tasked with different aspects of the process, as follows.

1. The National Institutes of Standards and Technology (NIST) is developing a privacy framework. Similar to its cybersecurity framework, NIST aims to create a voluntary framework as a tool for organizations to adopt to identify, assess, manage, and communicate about privacy risks.[75] By classifying specific privacy outcomes and potential approaches, the framework is intended to enable organizations to create and adapt privacy strategies, innovate, and manage privacy risks within diverse environments.[76]
   As part of its transparent approach, NIST is currently consulting with public and private sector stakeholders through various forms of outreach to collect feedback and aims to have a draft framework before the end of 2019.[77]
2. The National Telecommunications and Information Administration (NTIA) is developing a set of privacy principles to guide a domestic legal and policy approach. The NITA sought public comment on a proposed set of "user-centric privacy outcomes" and a set of high level goals.[78]

[72] UMSCA Article 19.8.

[73] U.S. International Trade Commission hearing on "United States-Mexico-Canada Agreement: Likely Impact on the U.S. Economy and Specific Industry Sectors," Inv. No.: TPA-105-003, November 16, 2018.

[74] See for example, the White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, February 2012, https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

[75] For more information on the NIST cybersecurity framework, see https://www.nist.gov/cyberframework.

[76] For more information on the NIST privacy framework, see https://www.nist.gov/privacy-framework.

[77] 83 FRN 56824, Docket No. 181101997-8997-01.

[78] 83 FRN 48600, Docket No. 180821780-8780-01. All comments submitted to NTIA can be found at: https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy.

3. The International Trade Administration (ITA) engages with foreign governments and international organizations such as APEC. ITA is focusing on the international interoperability aspects of potential U.S. privacy policy. ITA's role is to ensure that the NIST and NTIA approaches are consistent with U.S. international policy objectives, including TPA, and principles, such as the OECD framework and APEC CBPRs.

Like the EU and China, Commerce is seeking input through a public and private sector consultation process. However, unlike the EU or China, Commerce is expecting to create a voluntary privacy framework. Some observers question whether the Commerce approach is sufficient to result in strong privacy protections if it is not backed up by congressional action and federal legislation.[79]

Some suggest that Congress could lead a whole-of-government approach through new federal legislation. In the 115th Congress, then-House Committee on Energy and Commerce Ranking Member requested that the Government Accountability Office (GAO) examine issues related to federal oversight of internet privacy.[80] The January 2019 GAO report concluded that now is "an appropriate time for Congress to consider comprehensive Internet privacy."[81] GAO stated that "Congress should consider developing comprehensive legislation on Internet privacy that would enhance consumer protections and provide flexibility to address a rapidly evolving Internet environment. Issues that should be considered include what authorities agencies should have in order to oversee Internet privacy, including appropriate rulemaking authority."[82]

### U.S. State-Level Privacy Policies

Some U.S. states are advancing privacy rules in the absence of a coherent federal privacy policy. In June 2018, California passed the California Consumer Privacy Act of 2018, a broad digital privacy law that includes some similar consumer rights as in the EU GDPR, including clear and informed consent, the ability to opt out of data sharing, and the ability to access and correct personal information.[83] California's law contains a broader definition of "personal data" than the GDPR, covers information pertaining to households and devices, and has other distinctions. California's law goes into effect in 2020.[84]

U.S. companies voice concern that the California law may lead other states to pass their own laws, creating a patchwork of diverse state requirements and enforcement authorities. Differing state privacy policies and rules could increase compliance costs for organizations that function in multiple states and may impede interstate commerce, as a company based in one state may decline to serve a customer across state lines due to the complexity of complying with different or conflicting data requirements. Some businesses are seeking federal privacy legislation to harmonize state rules and preempt such problems.

[79] For example, see testimony from Laura Moy, Georgetown Law Center on Privacy & Technology, U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act*, 115th Cong., October 10, 2018

[80] Committee on Energy and Commerce Ranking Member Frank Pallone, Jr., letter to U.S. Government Accountability Office, February 27, 2017, https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/GAO.2017.02.27.%20Letter%20to%20GAO%20re%20Consumer%20Privacy.CAT_.pdf.

[81] U.S. Government Accountability Office, *Internet Privacy Additional Federal*, GAO-19-52, January 2019, p. 37, https://www.gao.gov/assets/700/696437.pdf.

[82] Ibid.

[83] California SB-1121 California Consumer Privacy Act of 2018, available at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB1121.

[84] For more information on the California law, see CRS Legal Sidebar LSB10213, *California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress*, by Wilson C. Freeman.

On the other hand, some stakeholders such as states' rights and privacy advocates seek to limit federal level involvement One coalition of consumer advocate organizations seeks to expand the California law further and supports state-level implementation and enforcement.[85]

## Stakeholder Perspectives

Recognizing the importance of protecting open data flows amid growing concerns about online privacy, some stakeholders seek to influence U.S. policies on these issues. In addition to submitting comments in response to NTIA and NIST requests and participating in their forums, multiple organizations issued their own sets of principles or guidelines, some referencing the EU GDPR. The U.S. Chamber of Commerce has also published model privacy legislation for Congress to consider.[86]

Though they vary in emphasis, these proposals share common themes.[87]

- transparency on what data is being collected and how it is being used;
- user control, including the ability to opt out of sharing at least some information and to access and correct personal data collected;
- data security measures, like data breach notification requirements; and
- enforcement by the FTC; FTC commissioners also voiced support for the agency as the appropriate federal enforcer for consumer privacy.[88]

But these groups also differ in some areas, such as whether, or to what extent, to include certain aspects included in the GDPR, such as the right to deletion (so-called "right to be forgotten"), requirements for data minimization, or extra-territorial reach. There is not consensus on whether the FTC should be given rule-making authority or additional resources, the enforcement role of states, or if an independent data protection commission is needed similar to EU DPAs.

Consistent with U.S. trade policy, industry groups generally point out the need to be flexible, encourage private sector innovation, establish sector- and technology-neutral rules, create international interoperability between privacy regimes, and facilitate cross-border data flows. Private sector stakeholders generally want to avoid what they regard as overregulation or high compliance burdens. These groups emphasize risk management and a harm-based approach, which they state keeps an organization's costs proportional to the consumer harm prevented.

[85] Letter to California State Legislature, December 3, 2018, https://advocacy.consumerreports.org/wp-content/uploads/2018/12/12.3.18-CCPA-Coalition-Letter-1-1.pdf.

[86] U.S. Chamber of Commerce, "U.S. Chamber Releases Model Privacy Legislation, Urges Congress to Pass a Federal Privacy Law," February 13, 2019, https://www.uschamber.com/press-release/us-chamber-releases-model-privacy-legislation-urges-congress-pass-federal-privacy-law.

[87] For example, see Access Now, letter to Chairman Thune, September 19, 2018; BSA, "Privacy Framework"; U.S. Chamber, "Privacy Principles"; Internet Association, "IA Privacy Principle for a Modern National Regulatory Framework"; Google, "Framework for Responsible Data Protection Regulation," September 2018; Verizon, "Privacy: It's time for Congress to do right by consumers," October 9, 2018; ITI, Framework to Advance Interoperable Rules (FAIR) on Privacy," October 22, 2018.

[88] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, *Oversight of the Federal Trade Commission*, 115th Cong., November 27, 2018.

On the other hand, some consumer advocates point to a need for baseline obligations to protect against discrimination, disinformation, or other harm. In general, consumer advocates believe that any comprehensive federal privacy policy should complement, and not supplant, sector-specific privacy legislation or state-level legislation.

# Shaping a Global Approach

Finding a global consensus on how to balance open data flows and privacy protection may be key to maintaining trust in the digital environment and advancing international trade. One study found that over 120 countries have laws related to personal data protection.[89] Divergent national privacy approaches raise the costs of doing business and make it harder for governments to collaborate and share data, whether for scientific research, defense, or law enforcement.

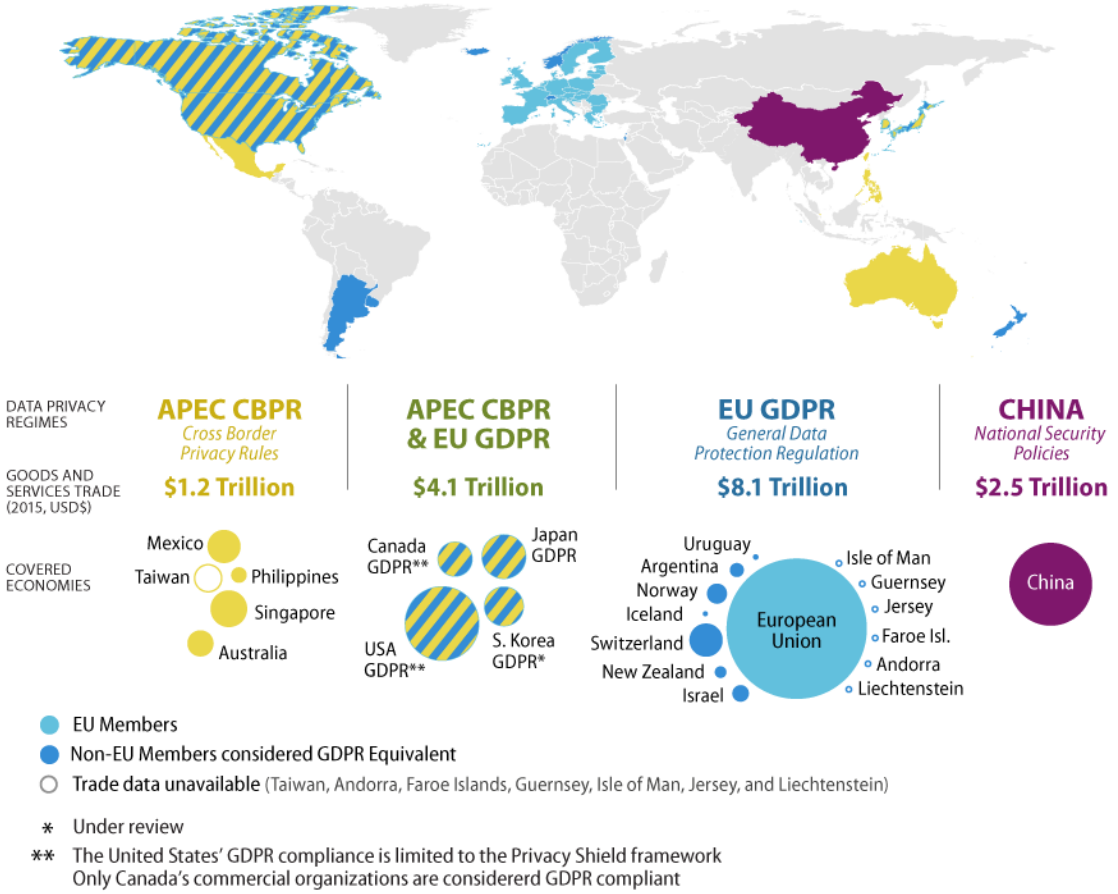
A system for global interoperability in a least trade restrictive and non-discriminatory way between different national systems could help minimize costs and allow entities in different jurisdictions with varying online privacy regimes to share data via cross-border data flows. Such a system could help avoid fragmentation of the internet between European, Chinese, and American spheres, a danger that some analysts have warned against.[90] For example, **Figure 2**, suggests the potential of an interoperability system that allows data to flow freely between GDPR and CBPR certified economies.

The OECD guidelines, G-20 principles, APEC CBPR, CPTPP and USMCA provisions demonstrate an evolving understanding on how to balance cross-border data flows, security, and privacy, to create interoperable policies that can be tailored by countries and avoid fragmentation or the potential exclusion of other countries or regulatory systems. The various trade agreements and initiatives with differing sets of parties may ultimately pave the way for a broader multilateral understanding and eventually lead to more enforceable binding commitments founded on the key WTO principles of non-discrimination, least trade restrictiveness, and transparency.

[89] C&M International, "Benefits of the APEC Cross-Border Privacy Rules," October 2018, https://www.crowell.com/files/20181001-Benefits-of-CBPR-System%20Guide_Oct%202018_final.pdf.

[90] The Editorial Board, "There May Soon Be Three Internets. America's Won't Necessarily Be the Best," *The New York Times*, October 15, 2018.

**Figure 2. Goods and Services Trade under Differing Data Privacy Regimes**




**Source:** CRS based on Comtrade data.

# Issues for Congress

## Future U.S. Trade Negotiations and Agreements

Congress may consider the trade-related aspects of data flows in trade agreements, including through close examination of these provisions during the congressional debate and consideration of legislation to implement the proposed USMCA. Issues include whether the agreements make progress in meeting TPA's related trade negotiating objectives and if the provisions strike the appropriate balance among public policy objectives. In addition, USTR's specific trade negotiating objectives for future agreements with the EU and Japan include establishing rules to protect cross-border data flows.[91] These future trade negotiations present challenges and provide opportunities for Congress to further engage USTR on the issues and to conduct oversight.

[91] USTR, "United States-Japan Trade Agreement (USJTA) Negotiations Summary of Specific Negotiating Objectives," December 2018; USTR, "United States-European Union Negotiations Summary of Specific Negotiating Objectives," January 2019.

## Global Approach

Congress may further consider how best to achieve broader consensus on data flows and privacy at the global level. Congress could, for example, conduct additional oversight of current best practice approaches (e.g., OECD, APEC) or ongoing negotiations in the WTO on e-commerce to create rules through plurilateral or multilateral agreements. Congress may consider endorsing certain of these efforts to influence international discussions and the engagement of other countries. Congress may want to examine the potential challenges and implications of building a system of interoperability between APEC, CBPR, and the EU GDPR.

Related issues are the extent to which the EU is establishing its system as a potential de facto global approach through its trade agreements and other mechanisms, and how U.S. and other trade agreements may ultimately provide approaches that could be adopted more globally.

## Impact on U.S. Trade

Congress may seek to better understand the economic impact of data flows and privacy regimes in other countries related to U.S. access to other markets and the extent to which barriers are being put in place that may discriminate against U.S. exporters. Congress may examine the lack of reciprocal treatment and limits on U.S. firms' access to some foreign markets.

Congress may consider the implications of not having a comprehensive national data privacy policy. Will the EU GDPR and China cybersecurity policies become the global norms that other countries follow in the absence of a clear U.S. alternative?

## Domestic Policy

Congress may enact comprehensive privacy legislation. In considering such action, Congress could investigate and conduct oversight of the Administration's ongoing privacy efforts, including requesting briefings and updates on the NTIA, NIST, and ITA initiatives to provide congressional feedback and direction and ensure they are aligned with U.S. trade objectives. Congress may also seek input from other federal agencies.

In deliberating a comprehensive U.S. policy on personal data privacy, Congress may review the GAO report's findings and conclusions. Congress may also weigh several factors, including:

- How can U.S. trade and domestic policy achieve the appropriate balance to encourage cross-border commerce, economic growth, and innovation, while safeguarding individual privacy and national security?
- What would be the impact of a new privacy regime on U.S. consumers and U.S. businesses, including large multinationals who must comply with different national privacy regimes, as well as small- and medium-sized enterprises with limited resources and technology expertise? Do U.S. agencies have the necessary tools to accurately measure the size and scope of cross-border data flows to help analyze the economic impact of different privacy policies, or measure the costs of trade barriers?
- How should an evolving U.S. privacy regime align with U.S. trade policy objectives and evolving international standards, such as the OECD Guidelines for privacy and cybersecurity and should U.S. policymakers prioritize interoperability with other international privacy frameworks to avoid further fragmentation of global markets and so-called balkanization of the internet?

- 

In addition, there are a host of other policy considerations not directly related to trade.

## Author Information

Rachel F. Fefer
Analyst in International Trade and Finance

## Disclaimer