

Data Flows, Online Privacy, and Trade Policy

Updated March 26, 2020

Congressional Research Service

<https://crsreports.congress.gov>

R45584



R45584

March 26, 2020

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 with expansion of both the amount of online data organizations collect and the level of global data flows. 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 Organisation 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. Recent U.S. and other trade agreements are establishing new enforceable trade rules and disciplines among subsets of trading partners.

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 different types of data, such as health records.

U.S. trade policy has sought to balance the goals of consumer privacy, security, and open commerce. The United States-Mexico-Canada Agreement (USMCA) is the first U.S. trade agreement to include rules and disciplines on privacy, cross-border data flows, and security. 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 multiple Members and committees have proposed 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

| | |
|---|----|
| Overview | 1 |
| Defining Online Privacy | 3 |
| Cross-Border Data Flows and Online Privacy | 3 |
| Balancing Policy Objectives | 5 |
| Multilateral Rules | 6 |
| WTO General Agreement on Trade in Services | 6 |
| WTO Plurilateral Effort | 6 |
| International Guidelines and Best Practices | 7 |
| OECD | 8 |
| G-20 | 8 |
| APEC | 8 |
| APEC CBPR | 9 |
| Expanding CBPR Beyond APEC | 10 |
| Foreign Government Policies | 10 |
| EU: Privacy First | 11 |
| U.S.-EU Privacy Shield | 11 |
| EU GDPR | 12 |
| Exporting Personal Data Under EU GDPR | 13 |
| Expanding GDPR Beyond the EU | 13 |
| China: Security First | 14 |
| Defining the U.S. Approach | 15 |
| Data Flows and Privacy in U.S. Trade Agreements | 16 |
| Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP/TPP-11) | 16 |
| Digital Economy Partnership Agreement (DEPA) | 17 |
| United States-Mexico-Canada Agreement (USMCA) | 17 |
| U.S. Federal Data Privacy Policy Efforts | 18 |
| Stakeholder Perspectives | 20 |
| Shaping a Global Approach | 22 |
| Issues for Congress | 23 |
| Future U.S. Trade Negotiations and Agreements | 23 |
| Global Approach | 24 |
| Impact on U.S. Trade | 24 |
| Domestic Policy | 24 |

Figures

| | |
|---|----|
| Figure 1. Digital Trade Restrictiveness Index | 11 |
| Figure 2. Goods and Services Trade under Differing Data Privacy Regimes | 23 |

Contacts

| | |
|--------------------------|----|
| Author Information | 25 |
|--------------------------|----|

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 the flow of digital data will increase global GDP by \$3,691 billion in 2020.¹ 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 nonpersonal 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 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.

In 2020, the world has an abundance of data but no global rules governing use or protection of that data. 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 United Kingdom (UK) referendum on continued European Union (EU) membership ("Brexit").² In addition, security concerns have been raised about data breaches, including that of credit reporting agency Equifax that exposed the sensitive financial and personal records of nearly 150 million Americans (and foreigners) or the Marriott breach which involved the personal data of 500 million hotel customers.³ The Department of Justice has since charged China's military in both cases.⁴

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.

¹ Gary Clyde Hufbauer and Zhiyao (Lucy) Lu, "Can Digital Flows Compensate for Lethargic Trade and Investment?" *Peterson Institute of Economics*, November 28, 2018.

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 Jackie Wattles and Selena Larson, "How the Equifax data breach happened: What we know now," *CNN Business*, September 16, 2017, and Taylor Telford and Craig Timberg, "Marriott discloses massive data breach affecting up to 500 million guests," *The Washington Post*, November 30, 2018.

⁴ Katie Benner, "U.S. Charges Chinese Military Officers in 2017 Equifax Hacking," *New York Times*, February 10, 2020.

Personal data is widely 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; the organization becomes responsible for protecting users' privacy and not misusing the information. Data privacy concerns may become more urgent with expansion of both (1) the amount of online information organizations access and collect, and (2) the level of global data flows.⁵

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 certain types of data, such as health records, although Congress is currently debating potential comprehensive national 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.⁶

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 and H.R. 5815 116th Congress, congressional committees held hearings on these topics,⁷ introduced multiple bills,⁸ and conducted oversight over federal laws on related issues such as data breach notification.⁹ Although data privacy crosses multiple committee jurisdictions, some have had greater focus on the topic than others. For example, the Chair and Ranking Member of the Senate Committee on Commerce, Science, and Transportation have each released their own version of proposed legislation that illustrate areas of differences and bipartisan alignment.¹⁰ Congress may review the digital trade chapter of the new U.S.-Mexico-Canada Agreement (USMCA) and the U.S.-Japan Digital Trade Agreement as examples of the

⁵ 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/>.

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

⁷ For example, 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; U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Examining Safeguards for Consumer Data Privacy*, 115th Cong., September 26, 2018; 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; and U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Policy Principles for a Federal Data Privacy Framework in the United States*, 116th Cong., February 27, 2019.

⁸ See for example, S. 2968, S. 142, or H.R. 4978.

⁹ 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.

¹⁰ See Consumer Online Privacy Rights Act (COPRA) (S. 2968) and staff draft of the United States Consumer Data Privacy Act (USCDPA), <https://www.commerce.senate.gov/2019/12/chairman-wicker-s-discussion-draft-the-united-states-consumer-data-privacy-act>.

current U.S. approach through trade agreements and as potential templates for future U.S. 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 may need to define personal data and differentiate between sensitive and nonsensitive 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.¹¹

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.¹²

The two Senate Commerce Committee draft bills mentioned previously generally align with the OMB definition, covering data that identifies or is linked or reasonably linkable to an individual or a consumer device, including derived data, but excluding de-identified or aggregated data, employee data, and public records. In addition, the policymakers each included provisions differentiating between sensitive and nonsensitive personal data. For example, sensitive personal data could include ethnic origin, political or religious affiliation, biometric data, health data, sexual orientation, precise geolocation data, and online activities. One concern is how potential U.S. legislation and subsequent regulation would define each of these terms.

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. One analysis estimated that digitally enabled trade was worth between \$800-\$1,500 billion globally in 2019.¹³ Effective and sustainable digital trade relies on data flows that permit commerce and communication but that

¹¹ 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.

¹² European Union General Data Protection Regulation, Article 4.

¹³ Christian Ketels, et al., “Global Trade Goes Digital,” *Boston Consulting Group*, August 12, 2019.

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.¹⁴

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

- block companies from using cloud computing to aggregate and analyze global data, or from gaining economies of scale,
- prevent companies from offering cross-border services to customers via the internet including entertainment and marketing,
- constrain e-commerce by limiting international online payments,
- hinder global supply chains seeking to use blockchain to track products or manage supply chains, customs documentation, or electronic payments,¹⁹
- impede the trading of crypto-currency, or
- limit the use of advanced technology like artificial intelligence that rely on collecting large data sets.²⁰

Business and Cross-Border Data Flows

- The world produces 2.5 quintillion bytes a day.¹⁵
- More than 50% of businesses globally rely on data flows for cloud computing.¹⁶
- One-third of total sales on the Etsy platform are international, relying on international data flows.¹⁷
- Data localization rules impeding data flows are the #1 digital trade barrier cited by U.S. firms.¹⁸

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.²¹ The extent of the impact of digital technologies on trade, however, depends in large part on open cross-border data flows.

¹⁴ A. Michael Spence, "Preventing the Balkanization of the Internet," The Council on Foreign Relations, March 18, 2018.

¹⁵ Thirani, Vasudha and Arvind Gupta, "The Value of Data." World Economic Forum, September 22, 2017, <http://www.weforum.org/agenda/2017/09/the-value-of-data/>

¹⁶ U.S. International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, Investigation Number: 332-561, August 2017.

¹⁷ Racheal Stelly, "Online Services Drive Exports, But Face Rising Trade Barriers," *Project DISCO*, April 3, 2019.

¹⁸ U.S. International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, Investigation Number: 332-561, August 2017.

¹⁹ Blockchain is a decentralized, distributed record or ledger of transactions in which the transactions are stored in a permanent database using cryptography. For more information on blockchain and international trade, see CRS In Focus IF10810, *Blockchain and International Trade*, by Rachel F. Fefer.

²⁰ 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.

²¹ WTO, "World Trade Report 2018: The future of world trade," https://www.wto.org/english/res_e/publications_e/

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.²² 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.²³

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. 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.²⁴ 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 and process data while protecting individuals' identities. The ongoing debate over employing encryption to protect individual security and privacy versus concerns about law enforcement and national security is related but distinct from cross-border data flows issues.²⁵

Some see an inherent conflict between online security, privacy, and trade; others believe that policies protecting all three can be coherent and consistent.²⁶ 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 seek proactive legislation to protect personal data. 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.²⁷ New rules by the Trump Administration that aim to allow patients to share their data online using common data standards are raising concerns about potential gaps in patient data privacy for entities such as app providers (e.g., Apple) who are not covered by HIPAA.²⁸ The Administration has begun an effort to devise an overarching

wtr18_e.htm.

²² U.S. International Trade Commission, *Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions*, Investigation Number: 332-561, August 2017.

²³ 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.

²⁴ 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.

²⁵ For more on encryption, see CRS Report R44642, *Encryption: Frequently Asked Questions*, by Chris Jaikaran or CRS Report R44187, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*, by Kristin Finklea.

²⁶ 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.

²⁷ For more information on HIPAA, see CRS Report R43991, *HIPAA Privacy, Security, Enforcement, and Breach Notification Standards*, by C. Stephen Redhead.

²⁸ Anna Wilde Mathews and Melanie Evans, "Sharing Your Digital Health Data: New Rules Ease Access," *The Wall*

data privacy policy (see “Defining the U.S. Approach”) and some Members of Congress are also considering possible approaches.

Multilateral Rules

There are no comprehensive multilateral rules specifically about privacy or cross-border data flows. 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) forum and the Organisation for Economic Co-operation and Development (OECD).

WTO General Agreement on Trade in Services

The World Trade Organization 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.²⁹ 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 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.³⁰

Efforts to update the multilateral agreement and discussions for new digital trade rules under the WTO Electronic Commerce Work Program stalled in 2017.³¹ 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

Over 80 countries, including the United States, are participating in ongoing WTO e-commerce negotiations aiming to establish a global framework and obligations to enable digital trade in a nondiscriminatory and less trade restrictive manner. Many stakeholders express hope that the negotiations will result in obligations, standards, and best practices regarding personal data protection and cross-border data flows. One notably large source and destination for digital trade, India, stated it will not join, preferring to maintain its flexibility to favor domestic firms, limit foreign market access, or raise revenue in the future.³²

Street Journal, March 9, 2020. For more information, see U.S. Department of Health and Human Services, “HHS Proposes New Rules to Improve the Interoperability of Electronic Health Information,” February 11, 2019, <https://www.hhs.gov/about/news/2019/02/11/hhs-proposes-new-rules-improve-interoperability-electronic-health-information.html>.

²⁹ The full text of the WTO GATS is available at https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm.

³⁰ WTO GATS Article XIV.

³¹ 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.

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

Multiple parties have submitted proposals outlining their positions and desired scope for the negotiations that reflect differences in their domestic policies and priorities (see “Foreign Government Policies”).³³ Proposals by the United States, China, and EU illustrate areas of potential overlap and disagreement.

- The **U.S.** proposal includes provisions to protect cross-border data flow and prevent data localization mandates. It also includes provisions from USMCA requiring parties to adopt or maintain a legal framework to protect personal information and encouraging the development of interoperability mechanisms.³⁴
- **China’s** proposal states that data flows and data storage should be subjects for exploratory discussions rather than solid commitments.³⁵ Regarding privacy, China states that the parties “should adopt measures that they consider appropriate and necessary to protect the personal information of electronic commerce users,” providing flexibility to governments but also not defining any principles or standards.³⁶ By excluding hard obligations, China’s proposal would essentially allow the country to maintain its highly restrictive internet regime.
- The **EU** proposes allowing cross-border data flows and prohibiting localization requirements, while allowing members to “adopt and maintain the safeguards they deem appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data.”³⁷ Some analysts see the exception as nullifying the commitment to cross-border data flows.

The U.S. Trade Representative’s (USTR’s) statement emphasized the need for a high-standard agreement that includes enforceable obligations.³⁸ 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.³⁹

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.

³³ All proposals can be found on the WTO online documents portal: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx.

³⁴ United States, *Joint Statement on Electronic Commerce*, WTO INF/ECOM/23, April 26, 2019.

³⁵ China, *Joint Statement on Electronic Commerce*, WTO INF/ECOM/19, April 23, 2019.

³⁶ Ibid.

³⁷ European Union, *Joint Statement on Electronic Commerce*, WTO INF/ECOM/22, April 26, 2019.

³⁸ 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>.

³⁹ “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.⁴⁰ 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.⁴¹ The updated guidelines identify specific principles for countries to take into account in establishing national policies. In 2019, members began the process to again review and update the guidelines.

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.”⁴²

Japan focused on data governance during its host year in 2019. The Osaka Leader’s Declaration recognized the importance of cross-border data flows, but also the challenges related to data protection and privacy.⁴³ To achieve “data free flow with trust” and strengthen the digital economy, the parties support interoperability between different frameworks.

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
 - be 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.

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.⁴⁴ Once the OECD publishes

⁴⁰ OECD, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” 1980, <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>.

⁴¹ OECD, “Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” 2013, <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>.

⁴² G-20 Digital Economy Ministerial Declaration, “G-20 Digital Economy,” August 24, 2018.

⁴³ G-20 Osaka Leaders’ Declaration, June 2019.

⁴⁴ APEC CTI Sub-Fora & Industry Dialogues Groups, Electronic Commerce Steering Group (ECSG), “APEC Privacy

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

APEC CBPR

The APEC Cross-Border Privacy Rules (CBPR), endorsed by APEC Leaders in 2011, is a privacy code of conduct, based on the 2005 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.⁴⁵ 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 allow 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.⁴⁶ Some stakeholders voice concern that the membership process is burdensome and costly, deterring many small and medium sized businesses.

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

Framework," APEC#205-SO-01.2, December 2005, <https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework>.

⁴⁵ <http://cbprs.org/>.

⁴⁶ More information on APEC CBPR accountability agents is available at <http://cbprs.org/accountability-agents/>.

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.

In the United States, the Federal Trade Commission (FTC) is the regulator and enforcement authority. U.S. accountability agents currently include TRUSTe and Schellman & Company, LLC.⁴⁷

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.”⁴⁸ 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 to countries outside of APEC could represent the next step toward consistent international rules and disciplines on data flows and privacy. Similarly, APEC CBPR could serve as a model for additional interoperability schemes between sets of developed and developing countries with shared regional interests or cultural norms. If other groups of countries create their own framework for interoperability, there is potential for broader interoperability between the varied systems.

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**).⁴⁹ Digital restrictions in the index cover policies such as data location requirements and limitations on cross-border data flows, financial investments, or e-commerce. The United States ranks 22 in this index, less restrictive than Brazil or France but more restrictive than Canada or Australia.⁵⁰ The relatively high U.S. score largely reflects financial sector restrictions.

The “restrictions on data” category covers data policies such as privacy and security measures; this category is included in the composite index. Looking specifically at the 64 countries’ data policies, Russia is the most restrictive country, followed by Turkey and China because of data

⁴⁷ <http://cbprs.org/accountability-agents/>.

⁴⁸ “U.S. recruiting countries to join APEC privacy system,” *World Trade Online*, February 7, 2019.

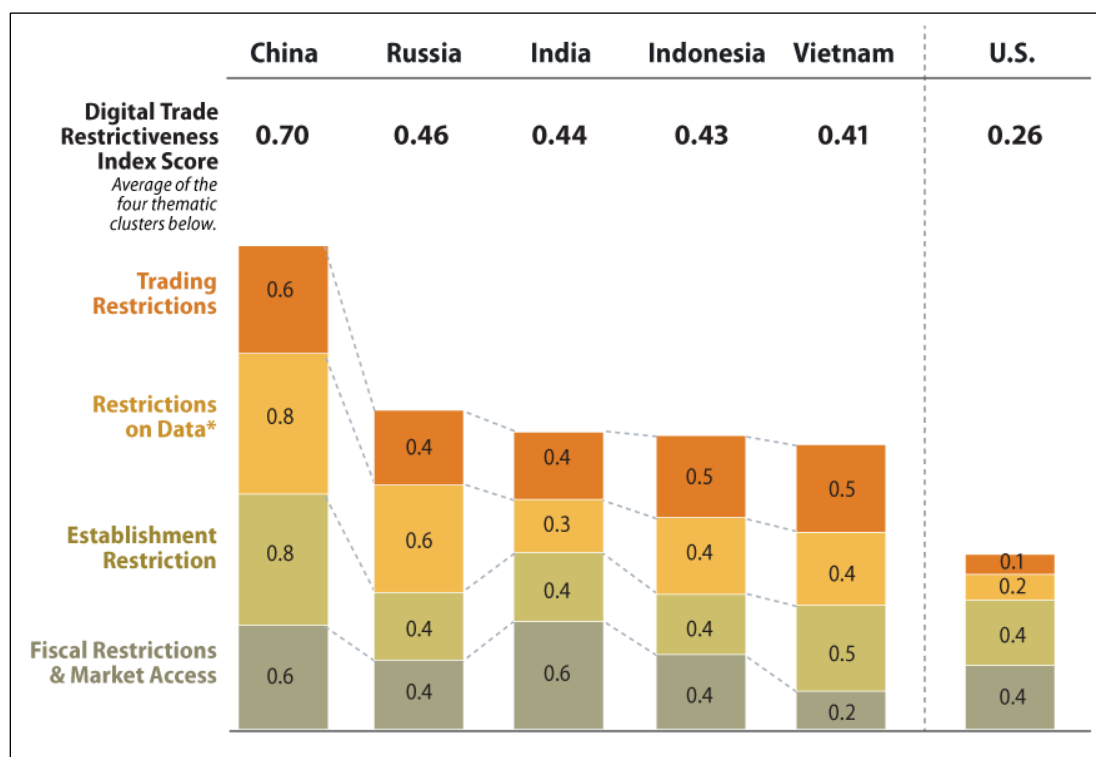
⁴⁹ ECIPE, “DTRI Trade Restrictiveness Index,” April 2018, <https://ecipe.org/dte/dte-report/>.

⁵⁰ The ECIPE index ranks individual countries and does not rank the EU as a single entity. Within the EU, there are areas of shared as well as nonshared competences among its member states; some measures in the index are the responsibility of individual EU member countries while others (such as data privacy regulations) are set at the EU level.

flow restrictions.⁵¹ Russia's policies include data localization, retention, and transfer requirements, among others. Turkey's comprehensive Data Protection Law also establishes requirements in these areas.⁵² 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.

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.⁵³ 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. In 2016, the EU and United States negotiated

⁵¹ Ibid, p. 54.

⁵² Turkish Personal Data Protection Law no. 6698 entered into force on April 7, 2016.

⁵³ 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.

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 and U.S. agencies, including the Department of Commerce and the FTC, and is reviewed by both parties annually.

As noted earlier, the United Kingdom (UK) withdrew from the EU on January 31, 2020. After the UK's transition period concludes at the end of 2020, the United States and UK may implement an agreement similar to the Privacy Shield to allow for cross-border data flows of personal data between the two countries.

EU GDPR

The EU's General Data Protection Regulation (GDPR), effective May 2018, establishes rules for EU members, with extraterritorial implications.⁵⁴ The GDPR is a comprehensive data 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 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

⁵⁴ 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, EU Data Protect.

complexities of complying with the GDPR and the threat of potential enforcement actions.⁵⁵ European Data Protection Authorities (DPAs) have received a range of GDPR complaints and initiated several GDPR enforcement actions. 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.⁵⁶ The Irish DPA is responsible for enforcement of the many multinational firms whose European headquarters are in Ireland, including Facebook and Google. In February 2020, the head of the Irish DPA stated that “six statutory inquiries were opened in relation to multinational technology companies’ compliance with the GDPR, bringing the total number of cross-border inquiries to 21.”⁵⁷

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;⁵⁸ or
3. A U.S.-based organization may enroll in the bilateral U.S.-EU Privacy Shield program for transatlantic transfer of personal data.⁵⁹

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 to be ready in case other countries introduce rules that imitate the GDPR.⁶⁰

⁵⁵ “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>.

⁵⁶ Laura Kayali, “France hits Google with €50 million fine for GDPR violation,” *Politico Pro*, January 21, 2019.

⁵⁷ Mark Scott, et al. “Morning Tech,” *PoliticoPro*, February 21, 2020.

⁵⁸ https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

⁵⁹ The U.S.-EU Privacy Shield has been challenged in the European Court of Justice (ECJ). For more information see, Bill Goodwin, “EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield,” *Computer Weekly*, December 19, 2019. Court case available at <http://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1839246>.

⁶⁰ For example, see Anick, Jesdanun, “Microsoft pledges to extend EU data rights worldwide,” May 21, 2018.

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.⁶¹ 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 in 2018 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 (the EU officially adopted its adequacy decision on Japan in January 2019).⁶² 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.⁶³

In advance of leaving the EU, the UK passed its Data Protection Act 2018 to align with GDPR.⁶⁴ The UK would need an adequacy determination by the EU in order to maintain cross-border data flows with the EU at the end of the transition period. The UK’s adequacy decision is not guaranteed and some European officials have raised concerns about some UK data protection policies; such uncertainty has, in turn, alarmed some UK and U.S. businesses that rely on sending data between UK and EU locations.⁶⁵ Google, for example, opted to move its British users’ accounts from storage in Ireland, which remains in the EU, to California (which has legal ownership of all Google EU data) in case the UK departs from GDPR in the future.⁶⁶

GDPR represents one part of the EU’s digital data strategy. The European Commission is in the process of building regulatory frameworks on data sharing and artificial intelligence, among other topics.⁶⁷ As with GDPR, the EU seeks to be a global leader in how governments regulate data. Some U.S. observers raise concerns that without a federal data policy, the United States may be missing an opportunity to set global precedents and maintain U.S. digital competitiveness.

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.⁶⁸ 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

⁶¹ 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.

⁶² 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.

⁶³ 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.

⁶⁴ <https://www.gov.uk/government/publications/data-protection-act-2018-overview>.

⁶⁵ Vincent Manancourt, “European Parliament takes aim at UK data protection regime,” *PoliticoPro*, February 12, 2020.

⁶⁶ Joseph Menn, “Exclusive: Google users in UK to lose EU data protection – sources,” *Reuters*, February 19, 2020.

⁶⁷ European Commission, Shaping Europe’s digital future: Commission presents strategies for data and Artificial Intelligence, <https://ec.europa.eu/digital-single-market/en/news/shaping-europes-digital-future-commission-presents-strategies-data-and-artificial-intelligence>.

⁶⁸ USTR, “2018 USTR Report to Congress on China’s WTO Compliance,” February 2019, p. 156.

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.⁶⁹

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.⁷⁰ 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 penalties 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.⁷¹ 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).⁷² 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.⁷³ 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.⁷⁴

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 to data-focused policies that restrict international trade and commerce to varying degrees. 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,⁷⁵ and the Trump White House's 2017 National Security Strategy.⁷⁶ 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

⁶⁹ Kelsey Munro, "China's social credit system 'could interfere in other nations' sovereignty,'" *The Guardian*, June 27, 2018.

⁷⁰ Jack Karsten and Darrell M. West, "China's social credit system spreads to more daily transactions," Brookings, June 18, 2018.

⁷¹ Yee Chung Seck and Thanh Son Dang, "Vietnam National Assembly Passes the Law on Cybersecurity," *Global Compliance News*, July 2, 2018.

⁷² Nigel Cory, "Vietnam's cybersecurity law threatens free trade," *Nikkei Asian Review*, August 15, 2018.

⁷³ INDUSLaw, "India: The Debate—Data Localization And Its Efficacy," September 17, 2018, mondaq.com.

⁷⁴ U.S. Trade Representative, *2018 National Trade Estimate Report on Foreign Trade Barriers*, 2018.

⁷⁵ <https://ustr.gov/sites/default/files/Digital-2-Dozen-Updated.pdf>.

⁷⁶ <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf>.

that the free flow of data is consistent with protecting privacy. 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.”⁷⁷ 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 entered into force at the end of 2018 among 11 Asia-Pacific countries.⁷⁸ 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 2017.

The electronic commerce chapter in TPP, left unchanged in CPTPP, includes provisions on cross-border data flows and personal information protection.⁷⁹ The text specifically states that the parties “shall allow the cross-border transfer of information.”⁸⁰ 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

⁷⁷ P.L. 114-26, Title I (b)(6)(C).

⁷⁸ 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.

⁷⁹ CPTPP Chapter 14, available at <https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf>.

⁸⁰ CPTPP Chapter 14 Article 14.11.

interoperability between data privacy regimes and encourages cooperation between consumer protection authorities.

Digital Economy Partnership Agreement (DEPA)

Although the United States is not a party to DEPA, the agreement is notable because it builds on the CPTPP. Three CPTPP parties, Singapore, New Zealand and Chile, concluded the DEPA in January 2020, but it is not yet in force.⁸¹ The agreement includes a series of modules covering measures that affect the digital economy. Module 4 on Data Issues includes binding provisions on personal data protection and cross-border data flows that build on the CPTPP. In addition to the CPTPP obligations, for example, DEPA encourages the adoption of data protection trustmarks for businesses to verify conformance with privacy standards. The agreement is an open plurilateral one that allows other countries to join the agreement as a whole, select specific modules to join, or replicate the modules in other trade agreements.⁸² New Zealand is to host APEC in 2021, providing the country an opportunity to promote the new agreement.

United States-Mexico-Canada Agreement (USMCA)

The USMCA revises, updates and replaces the trilateral North American Free Trade Agreement (NAFTA), and reflects the U.S. approach to data protection and cross border data flows.

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.⁸³

Building on principles in 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, and
- not prohibit or restrict cross-border transfer of information.

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.

USMCA Key Principles for Personal Information Protection

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

⁸¹ Ministers of Singapore, New Zealand and Chile, "Joint Ministerial Statement on the substantial conclusion of Digital Economy Partnership Agreement ("DEPA") negotiations," January 21, 2020, <https://www.mfat.govt.nz/assets/FTAs-agreed-not-signed/DEPA/Joint-Ministerial-Statement-on-DEPA-Substantial-Conclusion-FINAL.pdf>.

⁸² The released text of the DEPA may be found at <https://www.mfat.govt.nz/assets/FTAs-agreed-not-signed/DEPA/DEPA-Chile-New-Zealand-Singapore-21-Jan-2020-for-release.pdf>.

⁸³ 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/Text/19_Digital_Trade.pdf.

In general, the 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 recognizes APEC's CBPR as a "valid mechanism to facilitate cross-border information transfer while protecting personal information."⁸⁴

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 among 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 or the EU).⁸⁵ Cross-border data flows will likely be a key issue in future U.S.-EU trade negotiations.

U.S.-Japan Digital Trade Agreement. The U.S.-Japan Digital Trade Agreement, signed on October 7, 2019, covers rules on digital aspects of international commerce and parallels the USMCA. Considered an executive agreement, it took effect on January 1, 2020, without formal action by Congress.⁸⁶ Like USMCA, the agreement requires that the parties have a legal framework to protect personal information, have consumer protection laws for online commercial activities, and not prohibit or restrict cross-border transfer of information. The agreement promotes interoperability between privacy regimes, but does not refer to specific guidelines.

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. The Trump Administration is seeking to define an overarching U.S. approach on data privacy.⁸⁷ 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 Institute of Standards and Technology (NIST) released the first version of its Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework) on January 16, 2020.⁸⁸ Similar to its cybersecurity framework, the framework is a voluntary tool for

⁸⁴ USMCA Article 19.8.

⁸⁵ 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.

⁸⁶ U.S. Trade Representative, "FACT SHEET on U.S.-Japan Digital Trade Agreement," October 19, 2020. The full text of the agreement is available at https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.

⁸⁷ 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>.

⁸⁸ NIST, Privacy Framework, <https://www.nist.gov/privacy-framework/privacy-framework>.

organizations to adopt to identify, assess, manage, and communicate about privacy risks, whether within an organization or with customers or regulators.⁸⁹ By classifying specific privacy outcomes and potential approaches, the framework aims to enable organizations to create and adapt privacy strategies, innovate, and manage privacy risks within diverse regulatory environments. Through a risk and outcome-based approach, NIST intends the tool to be flexible and useful for organizations of all sizes and sectors. The framework does not define privacy, but provides common terminology for communication about data privacy risks, events or activities, and processes. U.S. officials can present the NIST tool internationally as a best practice similar to the cybersecurity framework. The privacy framework was created after extensive stakeholder consultation and is a living document as NIST continues to gather input and further develop the framework.

2. The National Telecommunications and Information Administration (NTIA) is developing a set of privacy principles to guide a domestic legal and policy approach. The NTIA sought public comment on a proposed set of “user-centric privacy outcomes” and a set of high-level goals.⁹⁰
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.

Unlike the EU or China, the Commerce initiatives create a voluntary privacy framework and principles to enable communication and best practices but not enforceable rules. The emerging Commerce tools are intended to work in different regulatory contexts, and are not meant to be a substitute for potential federal (or state) legislation or rule-making. 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.⁹¹

Some suggest that Congress could lead a whole-of-government approach through new federal legislation. Some stakeholders, including many U.S. businesses who operate globally, believe a common national standard on privacy would strengthen the U.S. position in international forums and provide an opportunity for clear U.S. leadership on the issue.

In the 115th Congress, then-House Committee on Energy and Commerce Ranking Member Frank Pallone, Jr. requested that the Government Accountability Office (GAO) examine issues related to federal oversight of internet privacy.⁹² The January 2019 GAO report concluded that now is “an

⁸⁹ For more information on the NIST cybersecurity framework, see <https://www.nist.gov/cyberframework>.

⁹⁰ 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>.

⁹¹ 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.

⁹² 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.

appropriate time for Congress to consider comprehensive Internet privacy.”⁹³ 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.”⁹⁴

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.⁹⁵ 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 entered into effect in 2020.⁹⁶ California’s Attorney General continues to release new rules to clarify the law and amendments for further changes have been introduced.⁹⁷

U.S. companies voice concern that the California law is leading other states to pass their own laws, creating a patchwork of diverse state requirements and enforcement authorities. For example, Washington state is considering a bill that has many similarities with California’s.⁹⁸

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 companies are using firewalls to build “digital borders,” selecting where to operate and who to serve. Some businesses are seeking federal privacy legislation to harmonize state rules and preempt such problems.

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.⁹⁹

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. The Global Data Alliance, a cross-industry coalition of multinational companies, was formed specifically to advocate for “policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade.”¹⁰⁰ Its members include a variety of sectors, including financial services, airlines,

⁹³ U.S. Government Accountability Office, *Internet Privacy Additional Federal*, GAO-19-52, January 2019, p. 37, <https://www.gao.gov/assets/700/696437.pdf>.

⁹⁴ Ibid.

⁹⁵ California SB-1121 California Consumer Privacy Act of 2018, available at http://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB1121.

⁹⁶ For more information on the California law, see CRS Legal Sidebar LSB10213, *California Dreamin’ of Privacy Regulation: The California Consumer Privacy Act and Congress*, coordinated by Eric N. Holmes.

⁹⁷ Katy Murphy, “Becerra posts new draft of California privacy regulations,” *PoliticoPro*, February 7, 2020; Eric J. Savitz, “If You Like CCPA, California’s New Privacy Law, Wait Until Version 2.0,” *Barron’s Magazine*, December 19, 2019.

⁹⁸ Joseph O’Sullivan, “Washington Passes Data Privacy Bill as Questions Remain,” *Seattle Times*, February 18, 2020.

⁹⁹ 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>.

¹⁰⁰ Business Software Alliance, “Global Data Alliance Promotes Sound Data Policy,” January 22, 2020, <https://www.globaldataalliance.org/>.

entertainment, and consumer goods, to demonstrate the foundational importance of cross-border data flows to U.S. firms.

In addition to providing input to NTIA and NIST processes, multiple U.S. businesses and 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.¹⁰¹

Though they vary in emphasis, these proposals share common themes:¹⁰²

- 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.¹⁰³

Industry groups' positions 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 extraterritorial 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. In general, industry seeks a federal standard to preempt a patchwork of differing state laws and requirements (see text box) and to provide a U.S. standard to promote internationally (see below). Despite general alignment across U.S. industry, there are points of disagreement when it comes to technical and legal language for implementation, often driven by how different sectors collect or use data (e.g., business-to-business software vendors or consumer platforms).

In addition, 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.

¹⁰¹ 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>.

¹⁰² 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.

¹⁰³ 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.

The various bills introduced illustrate key points of contention such as federal preemption and enforcement where Members would need to identify a compromise or consensus solution to move forward. How any U.S. legislation defines individual rights and specific legal terms (e.g., de-identified data, nonsensitive data) would not only shape U.S. domestic implementation but also the U.S. position in any international discussions.

Shaping a Global Approach

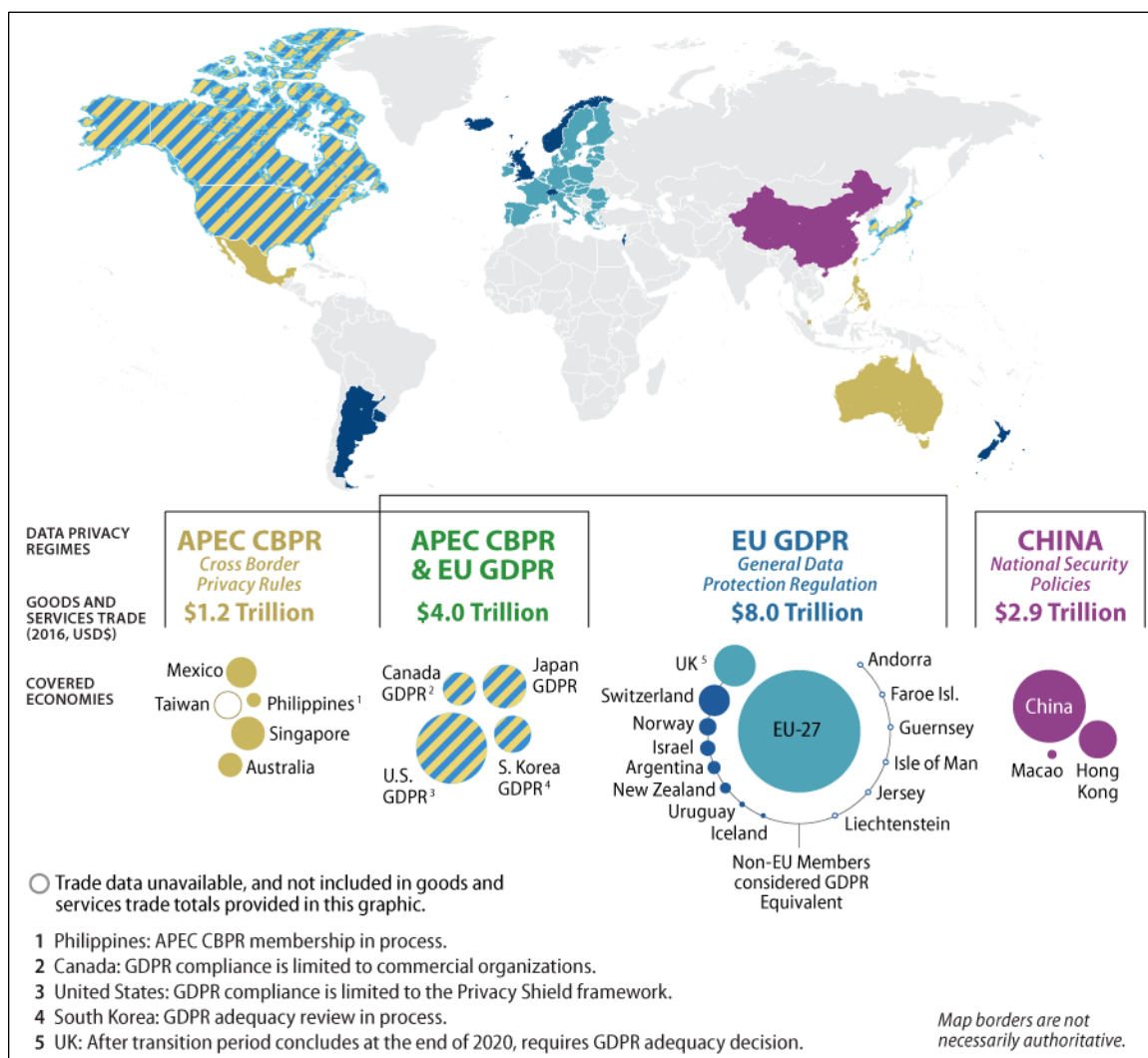
Finding a global consensus on how to balance open data flows and privacy protection may be key to maintaining trust in the digital environment and advancing international trade. One study found that over 120 countries have laws related to personal data protection.¹⁰⁴ Divergent national privacy approaches 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 nondiscriminatory 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 among European, Chinese, and American spheres, a danger that some analysts have warned against.¹⁰⁵ 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 FTA provisions such as those in the USMCA 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 nondiscrimination, least trade restrictiveness, and transparency. The ongoing WTO plurilateral negotiations provide an opportunity to achieve greater progress toward these goals.

¹⁰⁴ 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.

¹⁰⁵ 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.

Note: All USMCA partners are part of APEC CBPR, but only the United States and Canada have agreements with the EU.

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 oversight over ongoing, and future, WTO and bilateral trade negotiations, such as with the UK or EU. 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. TPA is authorized through July 1, 2021, providing Congress an opportunity to examine the current objectives and determine if they should be revised to specifically address pursuing a global approach to cross-border data flows.

Congress may consider whether the United States should seek additional narrow bilateral digital agreements with certain trading partners, similar to the U.S.-Japan agreement. On the one hand, such agreements could lock in U.S. digital norms in other parts of the globe, provide certainty to U.S. exporters, and strengthen the U.S. position in international trade negotiations and standards discussions. On the other hand, executive agreements like the U.S.-Japan digital agreement do not provide a role for congressional formal consideration.

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? Some have suggested that the EU could grant adequacy for cross-border data flows at a state-level for individual U.S. states that implement data protection laws (e.g., California).¹⁰⁶ Would such a move result in further fragmentation in the United States and create trade barriers between states or present a challenge to Congress's authority to regulate foreign commerce?

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?

¹⁰⁶ Sweeney Williams, "Could California Become an EU Data Privacy Darling?," *CMS Wire*, February 20, 2020.

- How would a new privacy regime affect U.S. consumers and businesses, including large multinationals who must comply with different national and U.S. state privacy regimes and small- and medium-sized enterprises with limited resources and technology expertise? Do U.S. agencies have the needed tools to accurately assess 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?
- Given that data privacy and protection are foundational to many policy areas, including trade, how (or who) should the United States be represented in international discussions on these topics?

In addition, beyond the scope of this report, 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

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.