EU Digital Policy and International Trade

March 25, 2021

Congressional Research Service
https://crsreports.congress.gov
R46732

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46732

March 25, 2021

Rachel F. Fefer
Analyst in International Trade and Finance

EU Digital Policy and International Trade

A "Europe fit for the digital age" is a top European Union (EU) priority and a key part of EU economic recovery efforts from the Coronavirus Disease 2019 (COVID-19) pandemic. Under the European Commission's digital policy roadmap, "Shaping Europe's Digital Future," the EU aims to strengthen the EU economy and improve the region's digital competitiveness, especially with the United States and China. The EU initiative may raise several issues for Congress, such as the impact on U.S. firms doing business in the EU and U.S. leadership in setting global digital rules and standards. The initiative may also offer the potential for partnership between the United States and the EU to address areas of common concern.

The EU has several digital efforts underway, including:

- The draft "Digital Markets Act (DMA)" that aims to establish competition rules for large online platforms designated as "gatekeepers" and specify a list of "do's and don'ts" among other requirements.
- The draft "Digital Services Act (DSA)" that seeks to modernize the 2000 E-Commerce Directive, which set the legal framework for online services in the EU, and set liability rules related to illegal online content and products, transparency, and other requirements for all online intermediary services.
- The enacted General Data Protection Regulation (GDPR), which took effect in 2018 and creates obligations on firms and rights for individuals regarding processing of personal data, including cross-border data flows.
- The proposed ePrivacy Regulation, still under debate, that is to impose requirements that ensure the privacy of electronic communications by both traditional telecommunications providers and messaging services.
- The draft "Data Governance Act" that seeks to regulate data and set the legal foundation for a single market for sharing industrial and nonpersonal data across the EU.
- The proposal on artificial intelligence (AI) that is to ensure "trustworthy AI" and a human-centric approach. Rules would categorize certain AI applications as high-risk, requiring ex ante approval for market access, while non-high-risk AI applications would be subject to a voluntary labeling scheme.

The transatlantic economy is key to the United States and the EU. In 2019, U.S. exports of information and communications technology (ICT) services to the EU was $31 billion, with potentially ICT-enabled services adding another $196 billion. Because the EU existing and proposed rules would apply to all organizations doing business in the EU, some stakeholders have raised concerns that the rules may hinder U.S. firms' ability to compete in the EU market, especially if the rules do not align with U.S. policies. In addition, the EU's head start establishing digital rules may allow it to set global norms in the absence of clear U.S. direction or multilateral agreements. Various ongoing efforts in the United States to address many of the technology issues that the EU is targeting (e.g., online competition, platform content, data privacy, and AI) create the potential for U.S.-EU cooperation both bilaterally and multilaterally.

Both political leaders and policy experts have recommended that the United States and the EU build a technology-focused alliance of like-minded democratic countries. Such an effort could help offset the rising digital and trade challenges from China as that country has sought to advance its authoritarian approach and set global guidelines and standards to regulate and control the internet. At the same time, greater U.S.-EU cooperation faces challenges amid different approaches, rules, and regulations in the digital realm, and increased tensions in the broader U.S.-EU relationship.

Congress may consider (1) the potential impact of the EU rules on the U.S. economy; (2) how EU policies may contrast or compare with U.S. policies; (3) conducting oversight on the domestic regulatory processes; and (4) examining opportunities for global leadership on digital norms. Congress may seek to work with the Biden Administration on trade or other initiatives to engage the EU on digital rules, including bilateral or multilateral efforts on these and other technology concerns. The Biden Administration has stated it seeks to improve U.S. relationships with its foreign partners, including the EU. It remains to be seen whether and how some key differences can be bridged.

Contents

Contacts

Introduction

A "Europe fit for the digital age" is a top European Union (EU) priority and a key part of EU economic recovery efforts from the Coronavirus Disease 2019 (COVID-19) pandemic. Under the European Commission's digital policy roadmap, "Shaping Europe's digital future," the EU aims to strengthen its economy and improve the region's digital competitiveness vis-à-vis the United States and China. As part of its strategy, the EU is pursuing regulatory, legislative, and legal efforts to achieve what some EU policymakers have termed "digital (or technological) sovereignty". The various EU initiatives under the strategy are wide-ranging—covering policies from artificial intelligence (AI) to competition to data privacy. Some U.S. firms have raised concern that the new rules may hinder their ability to compete in the EU market.[1]

Some policymakers and analysts note that the EU's head start in establishing digital rules may enable it to set global norms in the absence of clear U.S. policy or multilateral agreements.[2] Many of the EU initiatives are still in a proposal or draft form, allowing time for U.S. policymakers and other stakeholders to provide input. Contemporaneous efforts are underway in the United States to address similar technology issues targeted by the EU, creating potential opportunities for U.S.-EU cooperation. While their approaches and risk tolerances may vary, the U.S. and the EU share similar underlying democratic norms and values, opening the possibility of closer alignment or harmonization in some areas. U.S. and EU negotiators will need to find areas of agreement if they seek to build consensus and provide a counterweight to China and its authoritarian approach in the digital realm.[3] Various political leaders and policy experts have recommended that the United States and EU lead a technology-focused alliance of like-minded countries (see "Possible New Opportunities for U.S.-EU Cooperation?").

As Congress considers legislation to amend or establish new digital rules, it may consider (1) assessing the potential impact of the EU rules on the U.S. economy; (2) determining how EU policies may contrast or compare with U.S. policies; (3) conducting oversight on the domestic regulatory processes; and (4) examining opportunities for global leadership on digital norms. Congress may seek to work with the Biden Administration on trade or other initiatives to engage the EU on digital rules, including bilateral or multilateral efforts on these and other technology concerns.

At the same time, challenges persist to greater U.S.-EU cooperation. Different approaches, rules, and regulations in the digital realm and recent heightened tensions, and even distrust in the broader U.S.-EU relationship during the Trump Administration, contribute to these challenges. The Biden Administration has stated that it seeks to improve relationships with foreign partners, including the EU, and aims for greater international cooperation. It remains to be seen whether or how some key U.S.-EU differences can be bridged in the online sphere.

This report provides an overview of selected EU digital initiatives; analyzes how EU policies may contrast with or be similar to U.S. policies, particularly in trade agreements; and examines issues

[1] For example, Computer & Communications Industry Association, Position Paper on the EU Digital Markets Act, or Information Technology Industry Council, "ITI Views on the European Commission Proposal for a Digital Services Act (DSA)," March 10, 2021.

[2] For more information on global digital rules, see CRS Report R44565, *Digital Trade and U.S. Trade Policy*, coordinated by Rachel F. Fefer, and CRS Report R46198, *Internet Regimes and WTO E-Commerce Negotiations*, by Rachel F. Fefer.

[3] Aidan Powers-Riggs, "Covid-19 Is Proving a Boon for Digital Authoritarianism," *CNBC*, August 17, 2020, and Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism," *Freedom House*, 2018.

of possible congressional interest, including the impact of such initiatives on U.S. firms and U.S. leadership in trade agreement negotiations and rule-making on key technology issues.

This report will be updated as events warrant.

EU Digital Initiatives

As the head of the executive branch of the EU, European Commission President Ursula von der Leyen announced "A Europe fit for the digital age" as one of her six headline ambitions for the 2019-2024 term.[4] The European Commission's digital policy roadmap, "Shaping Europe's digital future," sets out various initiatives expected to form the core of the EU's digital agenda over the next several years. EU initiatives under consideration aim to forge a "fair and competitive" EU digital economy. Some of these initiatives build on previous work to integrate the EU member states through a Digital Single Market. These efforts led to changes such as the General Data Protection Regulation (GDPR), which took effect in 2018 and set rules and obligations regarding personal data.[5]

Ongoing EU efforts to further its single market seek to drive innovation, address online platforms, develop digital services, promote competition, and protect data. These efforts include:

- the draft "Digital Markets Act (DMA)" that aims to establish competition rules for large online platforms;
- the draft "Digital Services Act (DSA)" that seeks to set liability rules related to illegal online content and products, transparency obligations, and other requirements for all online intermediary services;
- the proposed ePrivacy Regulation that is to ensure the privacy of electronic communications;
- the draft "Data Governance Act" that seeks to regulate data sharing across the EU; and
- a proposal on artificial intelligence (AI) that is to ensure "trustworthy AI" and a human-centric approach.

Each proposed or draft regulation would take time to progress to enactment into EU law, potentially months or years, because it would require the approval of each member state (acting in the Council of the EU) and the European Parliament.[6] Whether each regulation once finalized and enacted will supersede national member state laws, and the amount of flexibility member states will have, remain to be seen. Apart from the initiatives included here, other programs under the EU digital policy roadmap address aspects such as workforce digital skills, infrastructure, green transition, digitalizing public services, or cybersecurity, among other topics.[7]

[4] Ursula von der Leyen, "A Union that strives for more, My agenda for Europe," 2019, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[5] For more information on the EU's Digital Single market strategy 2014-2019, see European Commission, "Shaping the Digital Single Market," October 29, 2020, https://ec.europa.eu/digital-single-market/en/shaping-digital-single-market.

[6] For more information on the EU legislative process, see https://ec.europa.eu/info/law/law-making-process/adopting-eu-law_en#:~:text=Most%20EU%20laws%20are%20adopted%20using%20the%20ordinary,in%20order%20for%20it%20to%20become%20EU%20law. Also see CRS In Focus IF11211, *The European Parliament and U.S. Interests*, by Kristin Archick.

[7] European Commission, "Shaping Europe's digital future," February 2020, at

Defining Digital Sovereignty

Starting in 2019, some European stakeholders began to voice the need for "digital sovereignty." In July 2019, a European Commission publication noted—

> "a global race for leadership in key digital technologies or enabling systems … has ensued … and it is increasingly characterized by international tensions and a growing 'geopoliticization' of digital technologies around the globe."[8]

It concluded that "a strong industrial and technological base will therefore be essential for European strategic autonomy" and the "ability of the EU and European stakeholders to shape rules and standards governing digital technologies, their use, and the companies producing and operating them, is crucial for its strategic autonomy."[9]

The EU does not have an official definition for "digital sovereignty" or "technological sovereignty." Some observers raise concern that the EU may aim to over-regulate new technologies and erect digital trade barriers, such as data localization requirements that would target U.S. technology firms who presently dominate the sector.[10] One European Parliament research paper defines "digital sovereignty" as Europe's ability to act independently in the digital world.[11] In clarifying his own view, EU Internal Market Commissioner Thierry Breton stated that "this is not about adopting a protectionist approach… Of course we are an open continent and we accept the technology of others, but under our rules."[12]

More recently, EU policymakers have talked about "open strategic autonomy," a term that reflects the desire for the EU to be able to act independently on the world stage, exerting leadership in line with EU interests and values in a wide range of areas, including in the trade, digital, and industrial policy spheres. The EU emphasizes that it will "remain a champion of openness and global cooperation," and in the trade realm, does not intend to pursue economic protectionism or isolationism.[13] EU officials have stated that the EU aims to have an open market with a competitive and level playing field, welcoming any firm that adheres to EU standards and regulations, which were developed to reflect EU values in how technology and data are used. EU standards and regulations, however, may not fully align with those of the United States, and could create additional burdens for U.S. firms in the EU market.

---

https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf, and https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en. For more information, see https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy.

[8] European Political Strategy Centre, "Rethinking Strategic Autonomy in the Digital Age," European Commission, July 18, 2019.

[9] Ibid.

[10] Discussions held during event, "Europe's search for digital sovereignty and post-COVID-19 geopolitics: Building a new US-EU digital dialogue?" Atlantic Council, June 25, 2020, and Charlene Barshefsky, former USTR, "EU digital protectionism risks damaging ties with the US," *Financial Times*, August 2, 2020.

[11] European Parliamentary Research Service, *Digital Sovereignty for Europe*, July 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[12] Vincent Manancourt, et al., "Breton: My approach on data isn't protectionist," *PoliticoPro*, January 28, 2020.

[13] European Commission, "Questions and Answers: An open, sustainable and assertive trade policy," February 18, 2021, https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_645.

Comparison to China and Internet Sovereignty

China expressed a desire for digital sovereignty before the EU began to discuss the concept. As early as 2010, China's State Council advanced the country's own view of "Internet Sovereignty" in a 2010 white paper:

> Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security.[14]

Analysts characterize China's version of "cyber sovereignty" or "internet sovereignty" as an organizing principle of internet governance. In its 2017 International Cooperation Strategy on Cyberspace, the Cyberspace Administration of China stated that:

> the principle of sovereignty… also includes cyberspace. Countries should respect each other's right to choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing.[15]

While some observers may see parallels to the EU's desire for digital sovereignty, China's version is more exclusive in nature with a focus on maintaining control and limiting external influences and actors. Some analysts contend that China's internet sovereignty initiative represents an assertion that the government has the right to fully control the internet within China including censorship and controlling information that is deemed a threat to social stability. Other critics of China's internet sovereignty policy view it as an attempt by the government to limit market access by foreign internet, digital, and high technology firms in China, to boost Chinese firms and reduce China's dependence on foreign technology.[16] China is also encouraging other, mostly developing, countries to support its model of internet sovereignty.[17]

Selected EU Technology Initiatives

Most of the initiatives discussed in this section are in the early stages of development in the EU legislative process. Progressing from a European Commission proposal to enactment into EU law takes time – whether months or years – because it requires the approval of each member state (acting in the Council of the EU) and the European Parliament. There are often different opinions among the member states, within the Parliament, and between the member states and the Parliament that must be reconciled.[18] As in the United States, throughout the process, EU officials

[14] Information Office of the State Council of the People's Republic of China, *The Internet in China*, Full Text in People's Daily, June 8, 2010, available at http://en.people.cn/90001/90776/90785/7017202.html.

[15] Cyberspace Administration of China, *International Strategy of Cooperation on Cyberspace*, March 1, 2017, at https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml.

[16] For more information on China's digital policies, see CRS Report R44565, *Digital Trade and U.S. Trade Policy*, coordinated by Rachel F. Fefer.

[17] William Chalk, "China's digital imperialism: Shaping the global internet," *SupChina*, July 2, 2019, at https://supchina.com/2019/07/02/chinas-digital-imperialism-shaping-the-global-internet/.

[18] For more information on the EU legislative process, see https://ec.europa.eu/info/law/law-making-process/adopting-eu-law_en#:~:text=Most%20EU%20laws%20are%20adopted%20using%20the%20ordinary,in%20order%20for%20it%20to%20become%20EU%20law. Also, see CRS In Focus IF11211, *The European Parliament and U.S. Interests*, by Kristin Archick.

may be lobbied by local constituents and private sector, civil society, or international stakeholders, including U.S. firms or policymakers.

Competition

The proposed Digital Markets Act (DMA) would establish competition rules for large online platforms that the EU designates as "gatekeepers."[19] The EU seeks to create a more equitable regulatory environment for small and medium-sized enterprises (SMEs) or new entrants by addressing the market concentration that results from the "network effect" that makes online platforms more appealing as more users are added. Because user data is often required for engagement with an online platform, EU officials note that the aggregation of such data can strengthen that platform's competitive position at the expense of SMEs or new market entrants. Therefore, data collection and usage, along with traditional competition metrics play a central role in determining market dominance. Executive Vice President of the European Commission Margrethe Vestager (with responsibility for EU digital policy) testified to the U.S. Congress about the need for new regulation and strong enforcement mechanisms to address the "significant harm to competition, innovation and ultimately to consumers" imposed by gatekeepers and their dual role as a platform operation and also competitor in certain markets.[20]

The criteria for defining a "gatekeeper" in the DMA draft includes digital platforms with European revenue of at least 6.5 billion euros (approximately $7.9 billion) or a market capitalization of at least 65 billion euros (approximately $79 billion), and which serve more than 10,000 active business customers and 45 million active end users in the bloc (approximately 10% of EU consumers). In addition, all companies that (1) operate in at least three EU countries, (2) control a digital ecosystem that rivals need to reach customers, and (3) maintain an entrenched market position would be included, thereby capturing online intermediaries that dominate specific sectors (e.g., online travel). Which firms are defined as gatekeepers would not be static, since the Commission could designate additional firms after conducting an investigation and companies would be able to challenge their designation at any time.

The DMA draft includes new ex ante rules[21] for platforms with a list of "do's and don'ts" for gatekeepers, identifying specific services that are allowed or prohibited. For example, platforms **must** allow business users to promote their offers and conclude contracts with customers outside the gatekeeper's platform and **must not** use data obtained from their business users to compete with those users. Another proposed rule would require platforms to notify the Commission of acquisition plans. Violations of the rules could result in fines of up to 10% of a company's total

[19] The Digital Markets Act (DMA), published December 15, 2020, by the European Commission, would establish competition rules for certain online platforms. European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act)*, COM/2020/842 final, December 15, 2020, at https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN. For more information, see European Commission, "The Digital Markets Act: ensuring fair and open digital markets," https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

[20] U.S. Congress, House Committee on the Judiciary, Subcommittee on Antitrust, Commercial, and Administrative Law, *Online Platforms and Market Power, Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google*, 116th Cong., July 29, 2020.

[21] Regulation is commonly referred to as an ex-ante ("existing before the event") government tool; competition rules and enforcement are commonly referred to as an ex-post ("after the fact").

worldwide annual revenue. In some cases, the Commission could impose behavioral or structural penalties (e.g., divestiture of certain businesses).

While the EU has pursued multiple anti-trust and competition cases against large technology companies, Commissioner Vestager views existing competition law enforcement in the EU as inadequate because it is "backward looking." The new rules would be "a way of introducing a forward-looking dynamic to complement what we do vigorously in enforcing competition law."[22] As noted, a new "competition tool" would allow for investigations of digital platforms that could evolve into gatekeepers in an effort to "future proof" the legislation; the tool may be expanded to allow for additional sectoral investigations. Furthermore, the DMA proposal aims for ongoing dialogue with gatekeepers to help regulators ensure that it is fair and effective.

Through the DMA, the Commission also seeks to harmonize online competition regulation across the EU, but the proposal remains subject to debate. Officials from the Commission, Parliament, and member states continue to examine the proposed regulation. Some of them have stressed the need to maintain flexibility by local authorities given the ex ante approach for rules and automatic classification of certain companies as gatekeepers. Some stakeholders have raised concerns that the proposal lacks a clear market objective or impact assessment of the specific harm(s) the regulation aims to address.[23]

Some member states are not waiting for the DMA to be finalized and are establishing their own competition regulations for digital platforms. For example, Germany is moving ahead with its own framework to create new online rules and provide competition authorities with tools to act before firms become dominant in a digital sector.[24] If other member states enact their own competition regulations, it could lead to greater fragmentation in the EU market. A fragmented EU market could make it harder for businesses, including U.S. exporters, to serve markets across the region as companies would need to comply with different rules in every EU member state. Whether or how the DMA would preempt or be compatible with member state regimes is not yet clear. German or other member state action in this regulatory sphere could bolster the Commission's case on the need to finalize and enact the DMA and strengthen the digital single market.

Platform Content

To address digital services platforms' responsibilities and liabilities, the European Commission is seeking to update and modernize the 2000 E-Commerce Directive[25] and it has proposed a new

[22] Javier Espinoza, "EU aims to stop online platforms getting too big for their boots," *Financial Times*, November 30, 2020. Examples of EU antitrust case: European Commission, "Antitrust: Commission sends Statement of Objections to Amazon for the use of nonpublic independent seller data and opens second investigation into its e-commerce business practices, November 10, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077; European Commission, "Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising," March 20, 2019, at https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770.

[23] PubAffairs Bruxelles, "Digital Markets Act: How to preserve innovation and competition in the EU digital economy?" January 25, 2021.

[24] Simon Van Dorpe, "Germany shows EU the way in curbing Big Tech," *Politico Pro,* January 13, 2021, and Simon Van Dorpe, "German lawmakers approve pioneering rules on Big Tech," *Politico Pro,* January 14, 2021.

[25] The e-Commerce Directive sets the legal framework for online services in the EU including for cross-border online services. European Commission, *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*, June 8, 2000, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000L0031.

Digital Services Act (DSA).[26] Like the DMA, the DSA is still in a relatively early stage of development and still is to be reviewed by the European Parliament and individual EU member states. Any finalized DMA or DSA rules would create harmonized regulatory frameworks across but the EU, but those regulations are not expected to go into effect before 2023.

In drafting the DSA, the Commission is aiming to "upgrade our liability and safety rules for digital platforms, services and products, and complete our digital single market."[27] The DSA includes rules for all online intermediary services doing business in the EU, but the requirements vary by company size and role in the digital marketplace with four distinct tiers identified in the draft. The greatest obligations would apply to "very large" platforms, defined as those with at least 45 million users (10% of the EU consumer base).

Generally, technology and social media companies act independently to determine what content should be deleted from or not permitted on their individual platform.[28] For example, the January 6, 2021, attack at the U.S. Capitol was, in part, publicized online. In the wake of this event, some companies decided to delete content based on their individual community rules or service contracts, as opposed to regulatory requirements, government censorship rules or legal orders.

Some EU leaders expressed an urgent need for clear regulation of online content. French Finance Minister said, "The regulation of the digital world cannot be done by the digital oligarchy."[29] In response, Internal Market Commissioner Thierry Breton, one of the leading forces behind the EU digital trade rules, wrote in an op-ed—

> We need to set the rules of the game and organize the digital space with clear rights, obligations and safeguards. We need to restore trust in the digital space. It is a matter of survival for our democracies in the 21st century…. What is illegal offline should also be illegal online.[30]

The proposed EU rules would focus on illegal online content, products, and services. The DSA imposes transparency reporting obligations on companies' actions to take down illegal content and provides safeguards for customers, but it does not include a general obligation for content monitoring. The draft maintains certain principles from the e-Commerce Directive, such as limited legal liability, protecting intermediaries from responsibility for the content on their services provided they make good-faith efforts to address problems, and country of origin supervision (as opposed to supervision by the country(s) of destination of services).[31] The top two tiers of intermediaries would be required to cooperate with so-called "trusted flagger" entities

[26] The Digital Services Act (DSA), published December 15, 2020, by the European Commission, would set rules for online intermediaries. European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, COM/2020/842 final, December 15, 2020, at https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN. For more information, see European Commission, "The Digital Services Act: ensuring a safe and accountable online environment," https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

[27] Laura Kayali, "Tech companies show their cards on content regulation," *Politico Pro,* January 7, 2021.

[28] For example, - Alex Agius Saliba comments, Member of the European Parliament S&D, at "Access Partnership The DSA: The Future of Content Regulation," Access Partnership webinar, January 13, 2021.

[29] Pierre-Paul Bermingham, "Merkel among EU leaders questioning Twitter's Trump ban," *Politico Pro,* January 11, 2021.

[30] Thierry Breton, "Thierry Breton: Capitol Hill — the 9/11 moment of social media," *Politico Pro,* January 11, 2021.

[31] Executive Vice-President Margrethe Vestager speech at "Building trust in technology," EPC Webinar, October 29, 2020.

who would identify illegal goods, services, and content online. Some EU member states and parties would have the regulation address broader harmful content and disinformation. These concepts lack a single EU-wide definition and may be context-specific, raising concerns among firms that seek clear rules and democracy and free speech advocates that fear a "slippery slope" of censorship.[32] Separate from the DSA, a new proposed EU regulation on preventing the dissemination of terrorist content online is expected to be formally adopted in 2021.[33]

In an attempt to protect consumers and combat dangerous, fraudulent, and counterfeit products, the DSA would strengthen existing transparency obligations by requiring independent auditors to conduct annual risk management assessments of the top tier ("very large") platforms. Further, the DSA would require both companies classified as "online" and "very large" platforms to verify their partners ("Know Your Business Customer" obligations), such as third-party sellers, and to provide greater transparency in their advertising, content moderation, and decision-making algorithms.

A proposed new cooperation mechanism in the DSA between member state regulators would aim to improve enforcement and further harmonization across the bloc. Fines would be imposable by a new EU-level body or by individual member states on entities in its jurisdiction. With no EU-wide definition of illegal content, it is unclear what the outcome would be if one member state requested that a platform based in another member state remove content that is legal in its home country.

In the midst of increased scrutiny and in anticipation of future regulation of online content, as well as to help minimize disruption to their business model, some large U.S. technology firms are proactively establishing new transparency mechanisms. For example, Google announced that its new Google Safety Engineering Center, located in Ireland, will serve as a "regional hub for Google experts working to tackle the spread of illegal and harmful content and a place where we can share this work with policymakers, researchers, and regulators."[34] Another example is Facebook, which established an Oversight Board to independently judge and "make binding decisions on what content Facebook and Instagram should allow or remove, based on respect for freedom of expression and human rights."[35]

Personal Data Privacy

The EU considers the privacy of communications and the protection of personal data to be fundamental rights, codified in EU law. Unlike the United States, the EU has had an overarching data privacy protection regulation since 1995 through its Data Protection Directive (DPD). The EU's General Data Protection Regulation, which took effect on May 25, 2018, and replaced the DPD, highlights some of the differences between U.S. and EU approaches to data privacy. [36] The GDPR identifies legitimate bases for data processing and sets out common rules for data retention, storage limitation, and recordkeeping. The regulation's extraterritorial nature has

[32] Laura Kayali, "Germany's recommendations on Digital Services Act, Digital Markets Act," *Politico Pro,* December 14, 2020; Bruna Martins dos Santos and David Morar, "Four lessons for U.S. legislators from the EU Digital Services Act," Brookings Institute, January 6, 2021.

[33] European Commission, "Commission welcomes political agreement on removing terrorist content online," press release, December 10, 2020, at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2372.

[34] Storey, Amanda, "GSEC Dublin: A content responsibility center for Europe," Google in Europe, January 27, 2021, at https://blog.google/around-the-globe/google-europe/gsec-dublin-content-responsibility-center-europe/.

[35] For more information on the Facebook Oversight Board, see https://www.facebook.com/pg/OversightBoard/about/?ref=page_internal and https://www.oversightboard.com/.

[36] For more information on General Data Protection Regulation (GDPR), see CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick.

implications for many U.S. businesses. The GDPR applies to (1) all businesses and organizations with an EU establishment that process (i.e., perform operations on) personal data of individuals (or "data subjects") 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 free) to individuals in the EU or monitor the behavior of individuals in the EU. Processing certain sensitive personal data is generally prohibited. A company or organization can be fined up to 4% of its annual global turnover or €20 million (whichever is greater) for noncompliance.

The GDPR created new rights for individuals regarding their personal data, such as the rights to allow or restrict data processing; access, rectify, and erase personal data; and data portability (i.e., to move one's data from one provider to another). As noted above, these rights follow the data when it leaves the EU, allowing EU individuals to hold foreign companies accountable for how their personal data is handled outside the EU. Under the GDPR, personal data may be transferred abroad only to countries with data protection regimes deemed "adequate" by the EU or under specific conditions defined in the regulation, such as binding corporate rules or standard contractual clauses.[37]

Some analysts have suggested updating the GDPR to make accommodations that promote innovation and the use of emerging technologies such as artificial intelligence (AI) that depend on large data sets.[38] Some EU officials have suggested creating regulatory sandboxes to allow for this sort of experimentation.[39] For now, it seems that the Commission will address AI and emerging technologies separately from the GDPR (see "Artificial Intelligence").

In addition, the EU is debating the ePrivacy Regulation to ensure privacy of electronic communications that would complement the GDPR's data protection requirements. The regulation would require traditional telecommunications providers, as well as messaging services (e.g., WhatsApp and SnapChat), to obtain explicit user consent for online tracking (use of cookies), and limit the amount of time that the tracking data may be stored. The regulation remains the subject of intense debate among European Commission officials, Parliament, and member states, with disagreements over its scope and how to define appropriate legal grounds for data use.

Technology Implications of Brexit

The United Kingdom (UK) formally withdrew from membership in the EU on January 31, 2020 (commonly termed Brexit). On January 1, 2021, after a transition period, the UK left the EU single market and customs union, shedding its rights and obligations as an EU member state and regaining control over its national regulatory and trade policy. Although UK regulatory frameworks have been aligned with the EU, Brexit allows the UK to diverge and makes the UK a "third country" from the EU perspective.

The UK is creating its own regulatory regime for the digital realm. The UK has proposed a new competition authority to oversee technology companies. A Digital Markets Unit within the Competition and Markets Authority would apply a code of conduct to companies with "strategic market status." The UK's draft legislation would address mandatory sharing and exchanging of data between tech companies in social media and e-commerce sectors and would require notifications of mergers and acquisitions activity. A separate Online Harms white paper proposes creating a legal duty of care requiring social media companies and search engines to take measures to remove user-generated content deemed illegal or potentially harmful material from their platforms. Violations of either of the proposed regulations could result in fines of up to 10% of annual global revenue.

[37] The European Commission has not granted a data protection adequacy decision to the United States. For more information on EU adequacy decisions, see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[38] Eline Chivot, "Is the EU's AI Policy Headed in the Right Direction? Evaluating EU AI White paper," Data Innovation webinar, July 15, 2020.

[39] Ibid.

The UK's Data Protection Act 2018 enacted the GDPR in UK law, aligning the UK's data privacy rules with the EU. Post Brexit, the EU has not made a final adequacy decision on the UK's data protection regime. The draft adequacy decision under consideration by the EU would allow open cross-border data flows between the UK and EU and the decision would be valid for four years. Many U.S. firms rely on such data flows to communicate with UK and EU customers, partners, and subsidiaries. The requirement to review the decision on a regular basis creates a level of uncertainty, especially if the UK considers changes in its data protection rules in the future. Going forward, the UK may consider trade-offs between maintaining rules that align with the EU to preserve EU equivalence or market access for British firms, or diverging to create a distinct UK regulatory environment that could align more with the United States or others in an effort to promote innovation and investment.

Note: For more information on Brexit, see CRS Report R45944, *Brexit: Status and Outlook*, coordinated by Derek E. Mix. For more information on the new UK rules, see UK Department for Business, Energy & Industrial Strategy, Department for Digital, Culture, Media & Sport, *New competition regime for tech giants to give consumers more choice and control over their data, and ensure businesses are fairly treated*, November 27, 2020, https://www.gov.uk/government/news/new-competition-regime-for-tech-giants-to-give-consumers-more-choice-and-control-over-their-data-and-ensure-businesses-are-fairly-treated, and UK Department for Digital, Culture, Media & Sport and Home Office, *Consultation outcome Online Harms White Paper*, April 8, 2019, https://www.gov.uk/government/consultations/online-harms-white-paper. For more information on the EU draft data adequacy decision see, European Commission, "Data protection: European Commission launches process on personal data flows to UK," press release, February 19, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.

Data and Cloud Services

After a public consultation period on an overarching data and cloud services strategy, in November 2020, the European Commission released its proposal for regulating data, the Data Governance Act.[40] Through this proposed policy, the Commission seeks to create "a new European way of data governance that is in line with EU values and principles," and provide a trusted data sharing alternative to using "Big Tech" platforms (e.g., U.S. companies like Google or Microsoft). The proposed rules set the legal foundation for a single market for data sharing across the EU with a focus on public and industrial, nonpersonal data while also encouraging "data altruism" by EU individuals to share their personal data for "the common good"; all data sharing by companies and individuals would be voluntary. According to the Commission, the proposed new measures could help generate economic benefits worth up to by up to €7-11 billion by 2028.[41]

The proposed Act identifies roles and rules for neutral "data intermediaries" to facilitate data sharing and identifies nine sectoral data spaces that would have varying approaches and requirements. Non-EU organizations would be able to participate in the data sharing provided they follow the EU requirements, which would include having a representative in the EU. Allaying initial fears by non-EU entities, the Act would not require that companies store data in the EU.

Under the proposal, data flows outside of the EU could be limited if a third country's data policies are assessed as insufficient and not equivalent to EU standards. The sharing of certain

[40] The proposed Data Governance Act, published November 25, 2020, by the European Commission, would set rules for data-sharing within the EU. European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)*, COM/2020/767 final, November 25, 2020, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.

[41] European Commission, *Data Governance Act Factsheet*, November 25, 2020, at https://ec.europa.eu/digital-single-market/en/news/data-governance-act and European Commission, *Proposal for a Regulation on European data governance (Data Governance Act)*, November 25, 2020, at https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act.

data with foreign country authorities could be restricted, as well as the number of people or companies who would be able to receive and reuse the data. Some stakeholders have raised concerns that the Data Governance Act could create an adequacy system for cross-border data flows that would require a lengthy approval process for international data transfers or destination country similar to GDPR and that such a process would not be scalable to a global level. Some analysts see potential conflicts between the Act and other existing EU rules, such as the GDPR.[42] In an attempt to ensure consistent policies and implementation across the EU, a new European Data Innovation Board would be created and include representation by the European Data Protection Board that oversees the GDPR.

The Data Governance Act would build on the Franco-German initiative GAIA-X, a nonprofit organization that aims to create a secure, federated platform for the data infrastructure used by cloud-service providers.[43] The nonprofit organization seeks to develop common standards, regulatory frameworks, and rules to establish secure trustworthy network infrastructure and an open, interoperable ecosystem for European cloud service users and companies. GAIA -X was launched by 22 companies and organizations (11 German and 11 French). It is open to all European companies and non-EU companies may join with limited rights. Large non-EU members include Amazon Web Services, Huawei, and IBM.

Artificial Intelligence (AI)

In February 2020, the European Commission released a white paper for public comment on AI setting out policy options to promote AI and to regulate potential risks.[44] The white paper proposes categorizing certain AI applications as "high-risk" that would require ex ante conformity assessment for market access while "non-high-risk" AI applications would be subject to a voluntary labeling scheme. The EU seeks to ensure "trustworthy AI," building on the ethics guidelines identified by an EU expert panel.[45] In differentiating the EU strategy, officials and EU documents describe the need for a human-centric approach that aligns with EU norms.[46] As the EU drafts its AI policy, a split is appearing between some member states, such as Germany, that prefer a strong regulatory approach and others, such as Denmark, that prefer self-regulation and voluntary practices along with standardization.[47]

In their responses to the white paper, U.S. stakeholders expressed concerns that new rules on AI could stifle innovation. Some of these stakeholders recommended instead that the EU adapt existing rules and promote "soft law" options such as industry-led standards and codes of conduct.[48] The former U.S. Chief Technology Officer under the Trump Administration stated "we

[42] Eline Chivot, "EU Data Strategy Has Worthwhile Goal, But Misses the Mark," Data Innovation, August 13, 2020, and Vincent Manancourt, "Schrems: 'Problematic' EU data law could undermine GDPR," *PoliticoPro*, November 24, 2020.

[43] For more information on GAIA-X, see https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

[44] European Commission, *On Artificial Intelligence - A European approach to excellence and trust*, February 19, 2020, at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[45] High-Level Expert Group on Artificial Intelligence set up by the European Commission, "Ethics Guidelines for Trustworthy Artificial Intelligence (AI)," April 8, 2019.

[46] Statements made during event "Is the EU's AI Policy Headed in the Right Direction? Evaluating EU AI White paper," Center for Data Innovation, July 15, 2020.

[47] Janosch Delcker, "14 EU countries urge Brussels to go easy on AI laws," *Politico Pro*, October 8, 2020 and Eline Chivot, "Germany Wants EU to Double Down on Idea That Would Hinder the AI Economy," Center for Data Innovation, October 9, 2020.

[48] For example, see Jason Oxman, "ITI's recommendations on the EU's Strategy on Artificial Intelligence,"

are particularly concerned that the EU's proposal clumsily attempts to place all AI technologies into one of two buckets… This approach is not particularly nimble and takes an unrealistic, all-or-nothing approach to AI regulation."[49]

The Commission plans to further clarify the definition of high-risk AI applications and release legislative proposals in 2021.

The European Union and Digital Service Taxes

The United States and more than 130 countries, comprising both members and nonmembers of the Organization for Economic Cooperation and Development (OECD), are negotiating policy recommendations in an attempt to update the global tax system and develop an international digital tax framework. With a lack of consensus to date on how to tax the digital economy, the Secretariat aims to conclude the negotiations in mid-2021.

While the EU agreed to postpone the imposition of any EU-wide Digital Service Taxes (DSTs) until OECD negotiations are complete, not all member states agreed. Some EU officials argue that the right to tax some of the profits of multinational corporations (MNCs) in certain "digital economy" sectors should be reallocated from the jurisdiction in which the MNC claims residence to the jurisdiction where the MNC's customers are located. Some member states have imposed unilateral DSTs on the gross revenues earned by digital economy MNCs. These taxes target certain MNC digital transactions with domestic businesses or online activities directed ultimately towards domestic users, even if the corporation does not have a physical presence in the country.

For example, France enacted a DST in 2019, applying a 3% levy on gross revenues derived from two digital activities in which French "users" are deemed to play a major role in value creation: (1) intermediary services, and (2) advertising services based on users' data. The law excludes certain services and applies only to companies above a certain annual revenues threshold globally and in France. France initially withheld implementing its tax in 2020, hoping that global negotiations would conclude by year-end. Without a clear international consensus, in November 2020, the French finance ministry notified companies of their DST charges for 2020. A U.S. Trade Representative (USTR) investigation under the Trump Administration concluded that France's DST discriminates against major U.S. digital companies and is inconsistent with prevailing international tax policy principles, and the Administration subsequently threatened tariffs on certain U.S. imports of French goods. Subsequent investigations into DSTs adopted by Italy, Austria, and Spain (as well as other non-EU countries) reached similar conclusions but the USTR did not propose specific actions in those cases. It is not clear if the Biden Administration will impose tariffs or other remedies if the OECD negotiations are not successful and countries move forward with individual DSTs.

Note: For more information, see CRS In Focus IF11564, *Section 301 Investigations: Foreign Digital Services Taxes (DSTs)*, by Andres B. Schwarzenberg. The USTR Section 301 investigations into Digital Service Taxes can be accessed at: https://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-digital-services-taxes.

EU Approach to Digital Trade in Free Trade Agreements

Overall, EU free trade agreements (FTAs) are not as comprehensive in digital trade and other areas as U.S. FTAs, although they share some common principles.[50] Similar to U.S. FTAs, EU FTA provisions generally prohibit customs duties on digital products and forced disclosure of source code; commit to nondiscrimination and transparency of domestic regulation; ensure technology choice and open internet access; allow for electronic signatures, authentication, and contracts; and require parties to have measures on consumer protection and spam. The EU stresses dialogues between FTA parties on multiple issues such as cooperation on matters related to cybersecurity and small and medium-sized enterprises. The EU also focuses on cooperation on

Information Technology Industry Council, February 17, 2020; Google, "Consultation on the white paper on AI – a European approach," May 28, 2020; and, Eline Chivot, "Response to the European Commission's Consultation on the on the White Paper on Artificial Intelligence," Center for Data Innovation, June 14, 2020.

[49] Jared Council, "U.S. Chief Technology Officer Criticizes EU's AI Plan," *Wall Street Journal*, February 19, 2020.

[50] For more information on U.S. FTAs and digital trade commitments, see CRS In Focus IF10770, *Digital Trade*, by Rachel F. Fefer.

some contentious subjects such as liability of intermediary service suppliers and personal data protection for which EU FTAs excludes hard obligations or commitments.

Unlike in U.S. FTAs, the EU does not include obligations on cross-border data flows or localization in its FTAs.[51] In contrast, as demonstrated by the EU's proposal in plurilateral negotiations at the World Trade Organization (WTO), the EU seeks to maintain regulatory flexibility on data flows and localization requirements. These requirements reflect the EU domestic policy emphasis on protecting personal privacy. The EU negotiating proposal contains obligations to ensure cross-border data flows and prohibitions on data localization, but also has a provision allowing parties 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."[52] Some analysts see the exception as nullifying the commitment to cross-border data flows (for more on WTO negotiations, see "Existing International Institutions").

U.S. FTA Approach to Digital Trade

In its own FTA negotiations, the United States has set new digital trade rules to promote open markets, digital trade, an open internet, and innovation while attempting to balance public policy goals that include protecting national security and privacy. U.S. and EU FTAs share many similar provisions (e.g., prohibiting customs duties on digital products; committing to nondiscrimination and consumer choice). However, U.S. FTA obligations are more extensive than those in EU FTAs.

The renegotiated North American Free Trade Agreement (NAFTA) illustrates the U.S. FTA approach as it addresses a wide variety of digital trade barriers. The U.S.-Mexico-Canada Agreement (USMCA), which replaced NAFTA on July 1, 2020, prohibits cross-border data flow limitations, localization requirements, technology transfer, or access to proprietary cryptography information. USMCA requires parties to establish civil and criminal procedures and penalties for trade secret theft, including cybertheft, the establishment of consumer protection laws, and a legal privacy framework to protect personal information that reflects international guidelines. To balance privacy and open data flows, the parties agreed to further develop and promote interoperability systems between privacy regimes. USMCA also recognizes risk-based approaches and the need for strengthened cooperation between governments on cybersecurity, and it encourages the use of open government data.

These themes are found in other U.S. trade agreements and proposals. The United States and Japan signed a digital trade agreement with provisions that parallel those of the USMCA. In addition, the U.S. proposal for the WTO plurilateral e-commerce negotiations echoes those agreements.

Note: For more information on the USMCA and U.S.-Japan agreements, see CRS In Focus IF10997, *U.S.-Mexico-Canada (USMCA) Trade Agreement*, by M. Angeles Villarreal and Ian F. Fergusson and CRS In Focus IF11120, *U.S.-Japan Trade Agreement Negotiations*, by Cathleen D. Cimino-Isaacs and Brock R. Williams.

U.S. Implications of EU Rules

Impact for U.S. Companies

The EU is a major consumer of U.S. digital services. In 2019, U.S. exports of information and communications technology (ICT) services to the EU was $31 billion, with potentially ICT-

[51] For examples of EU digital trade commitments in FTAs, see Agreement Between the European Union and Japan for an Economic Partnership, Chapter 8, Section F: Electronic commerce or Modernisation of the Trade part of the EU-Mexico Global Agreement Chapter on Digital Trade. The text of all EU trade agreements is available at https://ec.europa.eu/trade/policy/countries-and-regions/negotiations-and-agreements/.

[52] European Union, "Joint Statement on Electronic Commerce, EU Proposal for WTO Disciplines and Commitments Related to Electronic Commerce," WTO INF/ECOM/22, April 26, 2019.

enabled services adding another $196 billion.[53] Many U.S. companies are paying close attention to the EU's proposed new rules to understand the potential impact on their business and user bases. The EU approach to digital policy, including digital trade, generally is more regulatory and prescriptive than the U.S. approach. U.S. stakeholders often argue that such an approach stifles innovation and opportunities for growth. In general, the United States supports an open, secure, interoperable, and reliable internet, including the free flow of online information to promote a competitive and innovative environment.

In the absence of U.S. or international action, the EU could be setting de facto global rules or standards. For example, when the EU adopted the GDPR, some U.S. companies found it easier and cheaper to apply GDPR protections to all users worldwide rather than maintain different policies for users in different countries.[54] Companies could take the same approach to implementing changes required by new EU rules such as in the DSA or DMA. U.S. policymakers, the private sector, and civil society organizations are therefore voicing their opinions as the EU considers its various technology and digital initiatives.

U.S. firms generally oppose EU rules they view as targeting them and their business models, including a "gatekeeper" definition or digital services tax threshold that only applies to certain large firms, most of which are U.S.-based. The National Foreign Trade Council stated "The EU's focus on discriminatory approaches aimed specifically at innovative American companies threatens to undermine prospects for transatlantic cooperation on trade and technology."[55] Other groups voice concern that rules specific to large intermediaries may discourage innovation or scaling up by smaller firms.[56]

Beyond not wanting to be singled out, members of the U.S. technology industry have varied opinions on the various EU regulations and plans. Each firm's view depends on its own business model, market position, and perception of the effect the regulations might have. For example, regarding the draft DMA and DSA, a Google spokesperson stated, "We are concerned that they appear to specifically target a handful of companies and make it harder to develop new products to support small businesses in Europe."[57] Some analysts have raised concerns that the legislation is "anti-entrepreneurship" since it would raise compliance costs for small firms, possibly stifling innovation and growth. The App Association that represents mostly small firms stated, "App makers will suffer from the ripple effects this legislation will have on the whole ecosystem, making it more difficult to reach consumers and compete against big brands."[58]

Other U.S. firms are hoping new DMA and DSA rules create a more equitable marketplace or help them against specific competitors. Facebook said that the proposals are "on the right track to

[53] Cross-border services are often provided online or on the telephone. These services are considered ICT-enabled or potentially ICT-enabled (PICTE) services, and include an array of services, such as insurance and financial services; customer service; and business services like research, consulting, engineering, or cybersecurity. Data from Bureau of Economic Analysis, Interactive Table 3.3. U.S. Trade in ICT and Potentially ICT-Enabled Services, by Country or Affiliation ((A) (2006-2019)).

[54] Sahra English, Vice President, Public Policy, Mastercard, Remarks at Washington International Trade Association Conference, February 8, 2021.

[55] https://www.nftc.org/newsflash/newsflash.asp?Mode=View&id=236&articleid=4239&category=All.

[56] Victoria de Posson, "Digital Services Act: Ensuring a trustworthy and safe online environment while allowing freedom of expression," DISCO, January 20, 2021.

[57] Sam Schechner, "Tech Giants Face New Rules in Europe, Backed by Huge Fines," *Wall Street Journal*, December 16, 2020.

[58] "ACT The App Association Reacts to the European Commission's Digital Markets Act and Digital Services Act," *Daily Journal*, December 22, 2020.

help preserve what is good about the internet"[59] as the firm seeks to boost its position in part due to a confrontation with the Apple platform.[60] The Information Technology Industry Council, an industry association representing a diverse set of technology companies, took a more measured approach, stating "We fully support the goal of ensuring market access for innovative challengers, safeguarding consumer welfare and economic efficiency, but believe the Commission's proposal would benefit from further focus on a company's conduct and its interaction with users, rather than the size of a particular player, like revenues, users or the number of services it offers."[61] The same association identified specific concerns such as potential discrimination against selected platforms, disproportionate fines, and the ability for targeted firms to challenge complaints.

The ultimate impact on individual U.S. companies will depend on the details of the final rules. For example, revenue could decline if a company is required to invest resources to ensure compliance or make changes to its business model that disrupt its revenue stream, if the company exits the EU market because it decides that the required changes are too costly, or if the company incurs expenses to localize data storage in order to apply separate policies in the EU market. In addition, other U.S. firms may decide not to enter the EU market because of perceived costly, onerous obligations, forgoing potential revenue and profits. Other companies, especially niche U.S. SMEs, may not have to make any adjustments if they do not meet the specific criteria of new EU rules or if they offer their products and services via intermediaries that are EU-compliant. Should companies decide to invest the necessary resources in compliance, this may augment the EU's influence on global standards, especially if companies apply new EU-compliant policies and practices to all customers and businesses worldwide.

Like some countries who see EU rules as models worth imitating, individual U.S. states could decide to copy, in part or in whole, the EU rules, leading to greater fragmentation in the U.S. market. For example, California's privacy legislation is based in part on the EU's GDPR, and Virginia enacted similar, though less comprehensive, privacy legislation.[62] Maryland approved a tax on the revenue from digital advertisements, in part inspired by European digital service taxes.[63] These examples demonstrate the influence that new EU rules on the digital market could have on U.S. state regimes.

It is unclear if establishing digital rules would give the EU the global leadership role and digital sovereignty it seeks or if, conversely, new rules would stifle technology growth and innovation in the EU. In the industries where the EU has digital champions, such as Booking.com in online travel, there is concern that new rules could subject these sector-specific firms to the same

[59] Sam Schechner, "Tech Giants Face New Rules in Europe, Backed by Huge Fines," *Wall Street Journal*, December 16, 2020.

[60] Queenie Wong, "Facebook vs. Apple: Here's what you need to know about their privacy feud," *CNET*, February 10, 2021.

[61] Information Technology Industry Council, "ITI Reacts, Offers Initial Analysis to EU Proposals on New Rules for Internet Companies," December 15, 2020, at https://www.itic.org/news-events/news-releases/iti-reacts-offers-initial-analysis-to-eu-proposals-on-new-rules-for-internet-companies.

[62] California Privacy Rights Act is codified as Cal. Civ. Code §§ 1798.100-1798.199.100 and Virginia Consumer Data Protection Act, 2021 ch. 35 (to be codified at Va. Code Ann. §§ 59.1-571-59.1-581). For more information, see "GDPR v. CCPA: What You Need to Know," *American Marketing Association*, https://www.ama.org/pages/california-consumer-privacy-protection-act-what-you-need-to-know/ and Arent Fox, "Virginia Consumer Data Protection Act: Here Comes the Next State Privacy Law of the Land," *JDSUPRA*, March 8, 2021, athttps://www.jdsupra.com/legalnews/virginia-consumer-data-protection-act-2724869/.

[63] David McCabe, "Maryland Approves Country's First Tax on Big Tech's Ad Revenue," *The New York Times*, February 12, 2021.

constraints as the larger platforms that are active in multiple sectors and may compete against the more niche firms.[64]

U.S. Approach on Selected Technology Issues

Many U.S. firms welcome some amount of regulation to create clear rules of the road and regulatory certainty. For example, Google's chief executive officer stated

> I think it's an important regulation to think through and get right… What are the responsibilities on platforms? What is the contract we want to have? Where do there need to be clear processes, more transparency? I think all that makes sense to me. Thinking that through and tackling it, it's a worthwhile effort.[65]

While many in the private sector want clear and consistent rules, they are wary of sweeping regulations that could limit innovation and future technology development, force abrupt changes to business models, or mandate sharing of proprietary data with competitors without compensation.

While the EU pursues its "a Europe fit for the digital age" ambition, U.S. policymakers and others are moving forward with a less coordinated but broad review of technology policy. Below is a brief overview of some ongoing policy initiatives and debates.

Competition

Like their EU counterparts, U.S. policymakers have expressed an interest to ensure free and fair competition in digital markets. While the European Commission determined that existing competition law is insufficient and requires new rules and tools, the U.S. Congress, the Department of Justice (DOJ), and the Federal Trade Commission (FTC) have focused on using existing authorities and anti-trust laws to regulate the technology sector. The DOJ and FTC launched antitrust investigations into Google, Amazon, Facebook, and Apple ("Big Four" or "GAFA") in 2019,[66] and in October 2020, the DOJ and eleven Republican state attorneys general filed an antitrust lawsuit against Google related to its internet search services and advertising.[67] The 2020 lawsuit followed a bipartisan investigation by the House Committee on the Judiciary's Subcommittee on Antitrust, Commercial, and Administrative Law into digital markets competition. The investigation included multiple hearings and resulted in a report that concluded that some technology companies—including Google—had violated antitrust laws. The report proposed legislative and other reforms for further examination.[68] While many lawmakers of both parties agree that "Big Tech" raises unique competition issues, they have disagreed about the proper policy response.[69]

---

[64] Laura Kayali, "Booking CEO: We should not be regulated like Google," *PoliticoPro*, November 6, 2020.

[65] Richard Waters, "'Regulation can get it wrong': Google's Sundar Pichai on AI and antitrust," *The Financial Times*, December 23, 2020.

[66] For more information, see CRS Report R45910, *Antitrust and "Big Tech"*, by Jay B. Sykes.

[67] For more information, see CRS Legal Sidebar LSB10544, *The Google Antitrust Lawsuit: Initial Observations*, by Jay B. Sykes.

[68] U.S. Congress, House Committee on the Judiciary, Subcommittee on Antitrust, Commercial, and Administrative Law, *Investigation of Competition in Digital Markets*, committee print, prepared by Majority Staff Report and Recommendations, 116th Cong., 2020.

[69] *Compare id*. at 377-405 (proposing, among other things, structural-separation requirements for dominant platforms, interoperability rules, and presumptions of illegality for certain types of mergers), *with* Rep. Ken Buck, The Third Way, H. Judiciary Comm., Subcomm. on Antitrust, Commercial, and Administrative Law 8-18 (Oct. 6, 2020),

Platform Content

U.S. officials also have concerns about online content, though different policymakers have different concerns. In May 2020, former President Trump issued an executive order on the Communications Act of 1934, as amended (Section 230).[70] Section 230 creates federal immunity for providers and users of "interactive computer services," generally preventing them from being held liable for hosting content that someone else created.[71] This provision has allowed the growth of online platforms that host user-generated content. Some policymakers argue that Section 230 has allowed social media platforms to exert political bias in content removal and censorship to their detriment, while others voice concern that the provision has allowed false information, hate speech, and disinformation to spread online.[72]

In October 2020, the then Chairman of the Federal Communications Commission stated that he intended to move forward with a rulemaking to clarify Section 230, but later noted that he did not have sufficient time in his term to finish the process.[73] It is not clear if and how the Biden Administration will proceed. In December 2020, the FTC launched a study of social media and streaming platforms, specifically focusing on how such platforms "collect, use, and present personal information, their advertising and user engagement practices, and how their practices affect children and teens."[74] Separately, some Members of Congress and other stakeholders are scrutinizing the role of social media played in recent civil justice and political protests, as well as in the attack that disrupted the Electoral College vote count in the Capitol on January 6, 2021.[75]

In the 117th Congress, as in the 116th, multiple bills have been introduced to reform Section 230 (e.g., H.R. 277, S. 299). One issue may be that the United States has sought to limit the liability of internet service providers and information content providers in recent trade agreements (e.g., U.S.-Japan Agreement on Digital Trade and United States-Mexico-Canada Agreement) in line with Section 230.[76] Some Members have called for amending existing agreements and/or excluding such provisions in future trade agreements.[77]

In terms of illegal products, the USTR annually reports on markets, both physical and online, that facilitate substantial trademark counterfeiting and copyright piracy. In 2020, the report

---

https://buck.house.gov/sites/buck.house.gov/files/wysiwyg_uploaded/Buck%20Report.pdf (endorsing some but not all of the majority's recommendations).

[70] Executive Order 13925, "Preventing Online Censorship," 85 *Federal Register* 34079-34083, May 28, 2020.

[71] For more information, see CRS Legal Sidebar LSB10484, *UPDATE: Section 230 and the Executive Order on Preventing Online Censorship*, by Valerie C. Brannon et al.

[72] Todd Shields and Ben Brody, "Washington's Knives Are Out for Big Tech's Social Media Shield," *Bloomberg News*, August 11, 2020.

[73] FCC, *Statement of Chairman Pai on Section 230*, October 15, 2020, https://docs.fcc.gov/public/attachments/DOC-367567A1.pdf and Carrie Mihalcik, "FCC's Ajit Pai says he won't move forward on Section 230 rule-making," CNet, January 8, 2021.

[74] Federal Trade Commission, *FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information*, December 14, 2020, at https://www.ftc.gov/reports/6b-orders-file-special-reports-social-media-video-streaming-service-providers.

[75] Sheera Frenkel, "The storming of Capitol Hill was organized on social media," *New York Times*, January 6, 2021, and Christiano Lima and John Hendel, "'This is going to come back and bite 'em': Capitol breach inflames Democrats' ire at Silicon Valley," *PoliticoPro*, January 7, 2021.

[76] For more information, see CRS Legal Sidebar LSB10484, *UPDATE: Section 230 and the Executive Order on Preventing Online Censorship*, by Valerie C. Brannon et al.

[77] Senate Finance Committee letter to U.S. Trade Representative, December 18, 2020, at https://www.finance.senate.gov/imo/media/doc/Lighthizer%20letter%20US-UK%20tech.pdf.

highlighted the growth of digital platforms in facilitating trade in counterfeit and pirated goods and how such platforms have made it more difficult to detect such goods.[78] For example, it specifically included the Amazon marketplaces in multiple European countries. Domestically, the report noted that "Amazon partnered with the U.S. Government's National Intellectual Property Rights Coordination Center (IPR Center) on a joint operation to prevent counterfeit goods from entering the United States in an effort to protect American consumers."[79] The USTR report does not include any specific regulatory or penalty proposals.

Data Privacy

Unlike the EU, no single U.S. federal law comprehensively regulates the collection and use of consumers' personal data. While the U.S. Supreme Court has interpreted the Constitution to provide individuals a right to privacy, this right generally guards only against government intrusions. Given the limitations in constitutional law, Congress has enacted a number of laws designed to provide statutory protections of individuals' personal information. 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 to enforce broad online privacy protections. Adding to the complex patchwork of federal laws, some states have developed their own statutory frameworks for data protection.[80]

In previous sessions, several Members introduced comprehensive data privacy and data protection legislation and the topic may be revisited in the 117th Congress. A primary conceptual point of debate in data protection policy is whether to utilize a so-called "prescriptive" approach in which the law defines data protection rules and obligations (such as the EU's GDPR), or an "outcome-based" approach in which the law focuses on the outcomes of organizational practices, rather than defining what those practices should be. The Trump Administration pursued the latter approach: the National Institute of Standards and Technology (NIST) published its Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework) in January 2020 and the National Telecommunications and Information Administration (NTIA) is developing a set of "user-centric" privacy outcomes and goals that would underpin the protections that should be produced by any federal actions related to consumer privacy.[81]

U.S.-EU Privacy Shield

To bridge differences between U.S. and EU approaches to data privacy and protection, and to enable data transfers, the United States and the EU concluded data-sharing accords in both the commercial and law enforcement sectors. In July 2020, the Court of Justice of the European Union (CJEU, also known as the European Court of Justice, or ECJ) invalidated the most recent U.S.-EU commercial data transfer accord, the Privacy Shield Framework, which had been in force since 2016. The Privacy Shield had provided over 5,000 mostly small and

[78] U.S. Trade Representative, *2020 Review of Notorious Markets for Counterfeiting and Piracy*, January 14, 2021, at https://ustr.gov/sites/default/files/files/Press/Releases/2020%20Review%20of%20Notorious%20Markets%20for%20Counterfeiting%20and%20Piracy%20(final).pdf.

[79] Ibid, p. 20.

[80] For more information, see CRS In Focus IF11207, *Data Protection and Privacy Law: An Introduction*, by Stephen P. Mulligan and Chris D. Linebaugh and CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

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

mid-sized entities a mechanism to transfer EU citizens' personal data to the United States while complying with EU data protection rules. The CJEU found that Privacy Shield failed to meet EU GDPR data protection standards given the breadth of U.S. data collection powers authorized in U.S. electronic surveillance laws and the lack of redress options for EU citizens. The CJEU ruling creates legal uncertainty for many firms engaged in transatlantic trade. Although U.S. and EU officials have begun discussions on next steps to update or replace Privacy Shield, the CJEU decision demonstrates the potential difficulties that the parties face in attempting to overcome differences in their internet regimes and approaches to technology regulation.

Note: For more information on U.S.-EU data flows, see CRS In Focus IF11613, *U.S.-EU Privacy Shield*, by Rachel F. Fefer and Kristin Archick.

As EU and U.S. policies illustrate, 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.[82] The 2015 Trade Promotion Authority (TPA) (P.L. 114-26) includes a specific principal U.S. trade negotiating objective on "digital trade in goods and services and cross-border data flows."[83] According to the 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." For example, the USMCA and U.S.-Japan Digital Trade Agreement generally require that parties not restrict cross-border data flows and promote interoperability between data regimes.

Artificial Intelligence

Both the executive and legislative branches have actively shaped U.S. artificial intelligence (AI) strategy. In February 2019, President Trump issued an executive order announcing the American AI Initiative to create a national strategy on AI research and development (R&D) and deployment.[84] The order aimed to implement a "whole-of-government strategy in collaboration and engagement with the private sector, academia, the public, and like-minded international partners." It directed the federal government to pursue five pillars for advancing AI: "(1) invest in AI R&D, (2) unleash AI resources, (3) remove barriers to AI innovation, (4) train an AI-ready workforce, and (5) promote an international environment that is supportive of American AI innovation and its responsible use."[85]

Under the executive order, NIST is advancing fundamental and applied research and is involved in international standards discussions.[86] Congress reinforced NIST's role regarding AI when it passed, over a presidential veto, the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (P.L. 116-283; NDAA). The NDAA added AI to NIST's mission and tasked the agency with creating a voluntary risk management framework for trustworthy AI among other duties.[87] The executive order also called for guidance to federal agencies to inform regulatory and nonregulatory approaches for AI applications deployed outside

[82] For more information on data flows, see CRS Report R45584, *Data Flows, Online Privacy, and Trade Policy*, by Rachel F. Fefer.

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

[84] Executive Order 13859, "Maintaining American Leadership in Artificial Intelligence," 84 *Federal Register* 3967-3972, February 11, 2019.

[85] For more information on AI initiatives under the Trump Administration, see https://trumpwhitehouse.archives.gov/ai/.

[86] For more information on AI initiatives at NIST, see https://www.nist.gov/artificial-intelligence.

[87] P.L. 116-283 Title LIII, Sec. 5301.

of the federal government, leading to development of an Office of Management and Budget (OMB) memorandum on the issue.[88]

With a second executive order, President Trump aimed to promote AI use in the federal government.[89] Unlike the EU, the U.S. strategy does not focus on regulating this relatively new field. Like the EU, the strategy recognized the importance of values and established *Principles for Use of AI in Government* to guide adoption of AI while acknowledging separate frameworks for the fields of national security and defense.[90] Under the executive order, OMB is to publish a roadmap for policy guidance and recommendations for expanding AI expertise in government. For defense, the NDAA included provisions on the acquisition of ethically and responsibly developed AI.[91]

The NDAA contained additional AI-related provisions, including the direction to establish a National AI Initiative Office (NDAA Division E), which the Trump Administration announced in January 2021 as part of the White House Office of Science and Technology Policy, and a National AI Advisory Committee.[92] Other NDAA provisions on AI addressed topics such as training and R&D.[93]

It is unclear if President Biden will amend or revoke any of President Trump's executive orders or change any of the newly created federal guidance or offices related to AI.

Potential for U.S.-EU Cooperation

Because the United States and EU share many of the same democratic, liberal norms and values, as well as similar concerns about the digital realm, various stakeholders have expressed optimism about potential U.S.-EU cooperation and joint leadership on digital and technology issues. Due to the Biden Administration's emphasis on international cooperation, and the EU's commitment to working in multilateral forums on these issues and with the United States, in particular, there is an opportunity for two of the world's largest developed economies to work together. Some analysts question if the two parties can bridge their differences in technology and science-based regulatory approaches given, broadly speaking, the U.S. risk-based approach and the EU's more risk-averse approach with the application of the "precautionary principle."[94] Despite their differences, other stakeholders see potential for cooperation to build and promote baseline principles and rules for the digital world, both on a bilateral and multilateral basis, even if complete regulatory alignment or harmonization of the two systems is not feasible.

---

[88] Director Russell T. Vought, *Memorandum for the Heads of Executive Departments and Agencies: Guidance for Regulation of Artificial Intelligence Applications*, OMB, November 17, 2020.

[89] Executive Order 13960, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," 85 FR 78939 *Federal Register* 78939-78943, December 3, 2020.

[90] See Department of Defense, Ethical Principles for Artificial Intelligence, February 24, 2020; Office of the Director of National Intelligence Principles of Artificial Intelligence Ethics for the Intelligence Community, July 23, 2020, and Artificial Intelligence Ethics Framework for the Intelligence Community, July 23, 2020.

[91] P.L. 116-283 Title II, Sec. 235.

[92] Josh Mayo, "White House Launches National AI Initiative Office," MeriTalk, January 12, 2021.

[93] For more information on Department of Defense and AI, see CRS Report R45178, *Artificial Intelligence and National Security*, by Kelley M. Sayler.

[94] The precautionary principle states that if a product, an action, or a policy has a suspected risk of causing harm to the public or to the environment, protective action should be supported before there is complete scientific proof of a risk. In the absence of scientific consensus, the principle implies that there is a social responsibility to protect the public from potential harm.

Existing International Institutions

The United States and EU may consider taking advantage of existing international institutions to build common rules and norms based on their democratic values. Three of these forums are described below.

Organization for Economic Cooperation and Development (OECD)

An intergovernmental organization, the OECD describes itself as "a unique forum and knowledge hub for data and analysis, exchange of experiences, best-practice sharing, and advice on public policies and international standard-setting."[95] OECD meetings and working groups generate both binding and nonbinding guidelines, but the organization does not have an inherent enforcement mechanism and relies on member implementation. Digital taxation is already the subject of ongoing multilateral negotiations at the OECD. The OECD also serves as a venue for discussing emerging technologies. Through the OECD Regulatory Policy Committee and the Network of Economic Regulators, members are developing principles to address challenges presented by emerging technologies and to design "fit for purpose" regulation where appropriate.[96]

The United States and EU endorsed the OECD *Principles on AI*, which aim to promote innovative and trustworthy AI that respects human rights and democratic values.[97] The principles aim to set "practical and flexible" standards that allow for evolving technology and complement other OECD standards on privacy, digital security risk management and responsible business conduct. In addition, both the United States and EU are part of the Global Partnership on Artificial Intelligence (GPAI) that has created working groups of public and private sector, civil society organizations, and academia to address different aspects of AI.[98]

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.[99] Updated in 2013, the guidelines specify principles for countries to take into account in establishing national policies with an emphasis on interoperability.[100] As with AI and privacy, the OECD could serve as a venue to create common principles and best practices on other tech issues such as content moderation and platform competition.

Standards Development Organizations

The growth of international trade in ICT goods and services and emerging technologies relies on interoperability and international standards. According to the WTO Technical Barriers to Trade (TBT) Committee, which administers the TBT Agreement, WTO members are mandated to use relevant international standards as the basis for regulation, with some exceptions, and to not

[95] For more on the OECD, see OECD at http://www.oecd.org/about/.

[96] For more information on OECD "Better regulation and innovation," see http://www.oecd.org/gov/regulatory-policy/regulation-and-emerging-technologies.htm.

[97] OECD, *OECD Principles on AI*, June 2019, http://www.oecd.org/going-digital/ai/principles/.

[98] OECD Council, "Draft Memorandum of Understanding on the Hosting by the OECD of the Secretariat for the Global Partnership on Artificial Intelligence (GPAI)," C(2020)53, February 19, 2020.

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

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

create unnecessary obstacles to international trade.[101] Using international standards encourages transparency, innovation, and flexibility; such standards can evolve as technologies and new best practices develop.

Technology standards development organizations (SDOs) include entities such as the Institute of Electrical and Electronics Engineers, 3rd Generation Partnership Project (3GPP), and the International Organization for Standardization (ISO). By partnering together in the SDO context, the United States and EU could lead coalitions to ensure that new standards developed for emerging technologies, such as 5G or AI, are neutral, open, and interoperable as opposed to proprietary or favoring a single company or country. U.S.-EU-led coalitions could serve as a counterweight to China which has a growing presence in SDOs and is introducing a growing number of competing standards.[102] Nondiscriminatory international standards allow companies around the world to create, innovate, and compete on an equal level.[103] While U.S. and EU stakeholders and standards coalitions may compete with one another, by cooperating and abiding by the WTO principles, they can do so with fair market access.

Apart from technical standards, the United States and EU could create baseline standards to foster interoperability and cross-border data flows. For example, one group of transatlantic stakeholders created a flexible regulatory framework to address online content moderation.[104] On privacy, EU and U.S. partners could build on the OECD guidelines to agree on common principles such as a clearly defined "duty of care" standard rather than agree to a specific data regulations or require mutual recognition (or an adequacy determination). A joint U.S.-EU approach to these or other issues could create a de facto international standard, attracting other countries to align their national standards regimes to further interoperability and market integration to enhance the welfare of their own citizens and businesses.

World Trade Organization

Trade negotiations are a tool to could be used to create binding and enforceable rules and disciplines to promote international digital trade and bridge differing internet regimes. At the WTO, the United States, EU, and over 80 other parties are participating in ongoing negotiations on e-commerce aiming to establish a global framework and obligations that enable digital trade in a nondiscriminatory and less trade restrictive manner. The U.S. and EU have similar positions on many issues, including obligations on transparency, cooperation, and interoperability. On other issues, especially with regard to personal data protection and cross-border data flows, it is unclear if the two sides will be able to reconcile their different regulatory approaches to create common rules.

Despite their differences, the EU and U.S. proposals align more closely with each other than with proposals from China and other members that emphasize state control of online markets. Analysts

[101] Exceptions allowed "where such international standards or relevant parts would be ineffective or inappropriate, for instance, because of an insufficient level of protection or fundamental climatic or geographical factors or fundamental technological problems." WTO Technical Barriers to Trade Agreement Annex 3: Code of Good Practice for the Preparation, Adoption and Application of Standards, https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm.

[102] U.S.-China Business Council, "China in International Standards Setting," February 2020, at https://www.uschina.org/sites/default/files/china_in_international_standards_setting.pdf.

[103] For more information, see CRS Report R46198, *Internet Regimes and WTO E-Commerce Negotiations*, by Rachel F. Fefer.

[104] Annenberg Public Policy Center, "Freedom and Accountability A Transatlantic Framework for Moderating Speech Online," June 16, 2020, at https://www.annenbergpublicpolicycenter.org/feature/transatlantic-working-group-freedom-and-accountability/.

expect that the plurilateral WTO negotiators will have to decide between scope and inclusion.[105] A narrow agreement with limited scope and provisions, such as those focused on spam and e-commerce facilitation, would likely retain the greatest number of negotiating participants, including China, but could have less impact on digital trade if it does not address contentious issues such as data flows or emerging technologies. On the other hand, a high-standard broad agreement with deeper commitments, whether on privacy or online content moderation, may deter participants who are not yet willing or able to accept the obligations.

These and other international forums provide an opportunity for U.S.-EU cooperation to lead broader efforts to set common rules for emerging technologies and digital issues including online competition and content.

Possible New Opportunities for U.S.-EU Cooperation?

Some U.S. and EU government bodies have recently proposed new bilateral efforts to address digital technology challenges. In December 2020, the European Commission and the EU's High Representative for Foreign Affairs and Security Policy issued "*A New EU-U.S. Agenda for Global Change*" that is "based on our common values, interests and global influence."[106] The proposal includes multiple interdisciplinary issues including climate and public health. The proposed "joint EU-US tech agenda" includes creating a "transatlantic technology space [that] should form the backbone of a wider coalition of like-minded democracies with a shared vision on tech governance." The EU document specifically points to cooperation on AI, free data flow with trust, online platforms, competition, taxation in the digital economy, and standards. The EU proposal recommends establishing a new U.S.-EU Trade and Technology Council and having the transatlantic parties working together bilaterally to build and lead a broader coalition of partners.

In her address welcoming the new U.S. Administration, European Commission President von der Leyen reiterated her interest in cooperating with the United States. She stated,

> Together we could create a digital economy rulebook that is valid worldwide: From data protection and privacy to the security of critical infrastructure. A body of rules based on our values: human rights and pluralism, inclusion and protection of privacy.[107]

Von der Leyen reiterated support for a joint Trade and Technology Council as a "first step."

During his nomination hearing, Secretary of State Antony Blinken seemed to recognize a need to work with allies on technology norms. When asked about his strategy for confronting China's digital authoritarianism, Blinken responded,

> Bringing concerned countries together, … digital democracies together in an appropriate form I think is the place to start. And I don't want to minimize the challenge. We obviously have disagreements among democracies about a lot of profound questions about how

[105] A tiered agreement was brought up by multiple panelists during off-to-record panel discussions, AIG Global Trade Series 2019, https://www.aig.com/global-trade-series.

[106] European Commission, *Joint Commission to the European Parliament, the European Council and the Council: A New EU-U.S. Agenda for Global Change*, December 2, 2020, at https://ec.europa.eu/info/sites/info/files/joint-communication-eu-us-agenda_en.pdf.

[107] European Commission President von der Leyen, "Speech by President von der Leyen at the European Parliament Plenary on the inauguration of the new President of the United States and the current political situation," January 20, 2021, at https://ec.europa.eu/commission/presscorner/detail/en/speech_21_167.

> technology is used, so we've got some work to do just to get our own collective house in order.[108]

Several U.S. government plans that emphasize working with partners and allies on key technologies also provide an opportunity for cooperation with the EU. For example, the congressionally authorized Cyberspace Solarium Commission's national strategic approach to cybersecurity recommended that the United States "build a coalition of partners who share our values and use our powers to influence others."[109]

A report by the Senate Committee on Foreign Relations proposed "a constructive and concrete transatlantic agenda to defend shared interests and values" to counter multiple challenges posed by China.[110] With regard to technology, the report included four specific steps for the parties to: (1) prioritize areas where there are little to no regulatory obstacles for increased transatlantic cooperation on technology development (e.g., AI); (2) create a technology coalition of advanced democracies; (3) seek to harmonize regulatory practices in key areas (e.g., cybersecurity); and (4) take other steps to regain a competitive stance in the global technology race.

A bilateral U.S.-EU comprehensive FTA could also provide a forum to agree on new digital rules. Previous attempts at such negotiations under the Obama and Trump Administrations stalled due to differences on certain trade issues, not necessarily related to online technology.[111] The parties could consider a narrower digital trade agreement similar to the 2019 U.S.-Japan Digital Trade Agreement.[112] While the EU may not accept everything in the U.S. template, the parties could build on the agreement's provisions to include new obligations such as on competition, platform intermediaries, green tech, or emerging technologies in an effort to set new global standards.

Apart from a new bilateral trade agreement, the United States and EU could add their economic and political weight to existing agreements outside of the WTO that aim to shape new digital norms and standards. For example, the Digital Economy Partnership Agreement (DEPA), signed by Singapore, New Zealand and Chile, went into effect on January 7, 2021.[113] The agreement includes a series of modules covering measures that affect the digital economy such as cross-border data flows and digital identities. DEPA is an open plurilateral agreement that allows other countries to join the agreement as a whole, select specific modules to join, or replicate the modules in other trade agreements. Furthermore, it is a "living" agreement, allowing for the creation of new modules. For example, the parties explicitly included plans for deeper cooperation on emerging trends and technologies such as AI and competition, providing an opportunity for the United States and the EU to shape any obligations or new modules in these or other areas if they choose to join. U.S. and EU participation in DEPA could increase the agreement's influence in the global digital economy. Canada, a top U.S. trade partner, has held

---

[108] U.S. Congress, Senate Committee on Foreign Relations, *Nominations*, 117th Cong., January 19, 2021. Transcript at https://plus.cq.com/doc/congressionaltranscripts-6099730?0&searchId=RGXfZTkr.

[109] For more information, see CRS In Focus IF11469, *The Cyberspace Solarium Commission: Illuminating Options for Layered Deterrence*, by Chris Jaikaran and Solarium at https://www.solarium.gov/.

[110] U.S. Congress, Senate Committee on Foreign Relations, *A Concrete Agenda for Transatlantic Cooperation on China*, committee print, 116th Cong., November 2020, S. Prt. 116-46.

[111] For more information, see CRS In Focus IF11209, *U.S.-EU Trade Agreement Negotiations: Issues and Prospects*, coordinated by Shayerah I. Akhtar.

[112] The full text of the U.S.-Japan Digital Trade Agreement is available at https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text.

[113] For more information on DEPA, see https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement/.

exploratory discussions with the DEPA partners and is now conducting public consultations on the possibility of joining the DEPA.[114] The United States and EU may consider consulting with Canada on its decision or provide input as third parties.

In addition to internal government efforts, a number of civil society, industry and other stakeholders have proposed ideas for the United States and the EU to work together in the digital realm. In the face of rising digital and trade challenges from China's authoritarian approach, and the change in U.S. administrations, analysts representing an array of interests have proposed ways for the United States and EU to lead on new digital norms. The proposals often vary in scope; some suggest a narrow agreement on digital trade and standards, while others seeks to address broader, often inter-disciplinary, issues including democracy, export controls and investment screening, supply chain security, cybersecurity, emerging technology research and development and innovation, or internet governance. Some of the proposals focus on bilateral U.S.-EU cooperation while others seek to bring in certain additional third parties (e.g., UK, Canada, Brazil, India, and Australia); some proposals advise that the new forum be exclusive while others advocate for an open arrangement in which other countries could join. The structure of any new organization suggested varies as well, with some analysts proposing a formal trade agreement or partnership and others suggesting a more agile set of alliances, potentially with working groups that involve various countries or external experts. The proposals share a common tone and focus on aligning based on democratic principles, liberal values, and norms, and creating a coherent approach to address China's rise and the challenge it presents in the digital realm.[115]

Issues for Congress

The EU's technology initiatives and proposed new digital rules have multiple implications for U.S. policymakers. The EU rules have the potential to affect the United States economically by restricting U.S. companies' ability to conduct business in the EU or by forcing those firms to make changes. The timing of the EU proposals may limit U.S. policymakers' ability to provide an alternative model to shape global rules. At the same time, the EU proposals may open an opportunity for U.S.-EU cooperation on issues of shared concern related to digital trade and technology.

The EU proposals raise various issues that Congress may consider, including the following:

- With no multilateral rules on many of the digital issues the EU seeks to address, new EU rules may effectively set new de facto global standards, as firms and organizations strive for compliance to avoid being shut out of the EU market or

[114] Government of Canada, "Canada begins public consultations on joining the Digital Economy Partnership Agreement," *Global Affairs Canada news release,* March 19, 2021.

[115] Proposals include: Hans Binnendijk, et al. "The China plan: A transatlantic blueprint for strategic competition," Atlantic Council, March 22, 2021; Erik Brattberg and Ben Judah, "Forget the G-7, Build the D-10," *Foreign Policy,* June 10, 2020; IBM, "IBM Policy Lab: Bold Ideas for a Digital Society," September 13, 2020; Andrew Imbrie Ryan Fedasiuk, "An Alliance-Centered Approach to AI," CSET, September 2020; Robert K. Knake, "Weaponizing Digital Trade," Council on Foreign Relations," September 2020; Anja Manual, "US, Europe and UK must unite to keep Chinese tech at bay," *Financial Times,* October 5, 2020; Martijn Rasser, et al., "Common Code: An Alliance Framework for Democratic Technology Policy," Center for a New American Security, October 21, 2020; Sam DuPont, "Strengthening the Global Internet with a Digital Trade Agreement," German Marshall Fund, November 19, 2020; Steven Feldstein, "How Should Democracies Confront China's Digital Rise? Weighing the Merits of a T-10 Alliance," Council on Foreign Relations, November 30, 2002; Erik Brattberg, "Reinventing Transatlantic Relations on Climate, Democracy, Technology," Carnegie Endowment for International Peace, December 23, 2002; Joint letter by BSA, CCIA, ITI, IA, NFTC, "Promoting U.S. Global Leadership and Innovation: Digital Trade Priorities for the first 180 Days," January 21, 2021; and GMF Experts, "A Thirteen-Point Plan to Launch a New and Improved Transatlantic Alliance," German Marshall Fund, January 26, 2021.

penalized, and as other countries replicate the EU rules. Such developments could limit U.S. influence in future trade or standards negotiations. Congress may examine the EU proposals and engage the Biden Administration to help shape U.S. positions and responses, as the new USTR establishes its positions and priorities for ongoing and future trade negotiations. For example, in advance and during re-negotiations of the NAFTA, some Members of Congress, including the congressional Digital Trade Caucus, sent letters to the Administration and made public statements in support of adding new digital trade provisions in the updated agreement. Members may consider similar actions or introducing legislation (e.g., Sense of the House or Senate or a joint resolution) to express priorities for U.S.-EU discussions and to weigh in on the EU digital proposals. At the same time, Congress may seek to engage with counterparts in the European Parliament to provide input, such as through the policy discussions under the Transatlantic Legislators' Dialogue as the EU negotiates and finalizes the new rules.

- Establishing clear national digital rules and standards could provide an effective U.S. alternative to the EU model. Congress may decide whether and how to move forward with domestic policy in contentious technology areas, including Section 230 reform, amending and/or enforcing antitrust and competition rules, comprehensive personal data privacy rules and other emerging digital issues. Any reforms to Section 230 may impact a wide spectrum of U.S. stakeholders and would require Congress to weigh competing equities and policy objectives beyond international trade, as in prior Section 230 reform efforts.[116]
- U.S. firms doing business in Europe would be required to comply with any new EU rules if and when they come into effect, which may affect their business model, market share, and economic growth outlook. Congress may examine the potential impact of the EU rules on U.S. firms' ability to innovate, engage in digital trade, and contribute to the U.S. economy. Congress could consider asking the U.S. International Trade Commission to assess the likely impact of the new rules on the U.S. economy as the agency does for proposed trade agreements.
- The current TPA is authorized through July 1, 2021, providing Congress an opportunity to examine current U.S. negotiating objectives and determine if they should be revised.[117] Congress may debate whether current Section 230 protections should continue to be included in U.S. trade agreements. During the last TPA renewal, Congress added a reference to global value chains in its principle trade negotiating objectives on trade in services. Congress may consider adding objectives to specifically address pursuing a global approach to emerging technologies and issues affecting the digital market, including through international standards bodies or trade agreements or may hold hearings to further examine these issues.
- Congress may consider whether or not to recommend that the Biden Administration pursue a comprehensive FTA with the EU or a narrow digital agreement with the EU. If pursuing a phased or partial approach, Congress may examine if, and how, negotiators should update the existing template of the U.S-Japan Digital Trade Agreement or include a broader array of issues (e.g.,

[116] For more information on Section 230 reform, see CRS Legal Sidebar LSB10306, *Liability for Content Hosts: An Overview of the Communication Decency Act's Section 230*, by Valerie C. Brannon.

[117] For more information on TPA, see CRS Report R43491, *Trade Promotion Authority (TPA): Frequently Asked Questions*, by Ian F. Fergusson and Christopher M. Davis.

- platform competition, green technology). Similarly, Congress may study whether the United States should consider joining the DEPA, alone or in conjunction with the EU. Congress may seek consultation on the idea through public hearings.
- Congress could conduct oversight of current international discussions on technology rules, norms, and best practices (e.g., OECD), ongoing negotiations in the WTO or new bilateral forums created by the United States and EU. Congress may consider endorsing certain of these efforts to influence discussions and shape the potential engagement of other countries. Similarly, Congress could hold hearings on U.S. government and private sector involvement in standard-setting, pass legislation supporting enhanced U.S. involvement in standards-setting bodies, or examine how to build common approaches or coordination with the EU vis-à-vis China in international standards discussions.
- If new bilateral forums or agreements are to be pursued, Congress may identify specific guidance to identify priorities or set boundaries. Congress may consider how U.S. and EU policymakers can overcome the challenges that have traditionally impeded greater U.S.-EU cooperation (e.g., EU precautionary approach to regulation as opposed to risk-based approach or primacy of data privacy as opposed to the right to free speech).

Author Information

Rachel F. Fefer
Analyst in International Trade and Finance

Disclaimer