Before the
Office of the United States Trade Representative
Washington, D.C.

In re	
Request for Comments on the U.S.-EU Trade and Technology Council (TTC) Global Trade Challenges Working Group	Docket No. USTR–2024–0017

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

In response to the Office of the United States Trade Representative (USTR)'s request for comment on U.S.-EU Trade and Technology Council (TTC) Global Trade Challenges Working Group,[1] published in the Federal Register at 89 Fed. Reg. 72,696 the Computer & Communications Industry Association ("CCIA")[2] submits the following comments.

I. Introduction

The TTC, in its initial conception, represented a promising venue for the United States and European Union to cooperate both on areas of agreement as well as address differing perspectives relating to trade and technology. The Global Trade Challenges Working Group (Working Group 10, or WG10) served as a potential venue to incorporate both areas of collaboration and contention. Working Group 10 could have been leveraged to address, in tandem, laws and regulations from non-market economies that harm U.S. and EU interests, while also bridging policy and regulatory differences that, if left unattended, could embolden rivals like China.

[1] https://www.govinfo.gov/content/pkg/FR-2024-09-05/pdf/2024-19881.pdf.

[2] CCIA is an international nonprofit membership organization representing companies in the computer, Internet, information technology, and telecommunications industries. Together, CCIA's members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue. CCIA promotes open markets, open systems, open networks, and full, fair, and open competition in the computer, telecommunications, and Internet industries. A complete list of CCIA members is available at http://www.ccianet.org/members.

In the initial TTC Inaugural Joint Statement's Statement on Global Trade Challenges, the United States and EU listed a series of non-market practices they sought to address, including: "forced technology transfer; state-sponsored theft of intellectual property; market-distorting industrial subsidies, including support given to and through SOEs, and all other types of support offered by governments; the establishment of domestic and international market share targets; discriminatory treatment of foreign companies and their products and services in support of industrial policy objectives; and anti-competitive and non-market actions of SOEs."[3] These commitments were coupled with an acknowledgement that "domestic measures that each takes on its own can play a critical role in ensuring that trade policy supports market-based economies and the rule of law."[4] Since then, subsequent TTC statements have included commitments to continue collaborating on a series of diplomatic priorities[5] and coordination with third-party countries regarding China's "non-market policies and practices in the medical devices sector."[6]

The actions taken so far through the TTC as a whole have secured some policy successes in promoting connectivity in Latin America, the Caribbean, the Asia-Pacific, and Africa,[7] as well as cooperation responding to Russia's invasion of Ukraine through "sanction-related export restrictions and combating foreign information manipulation and interference (FIMI) and disinformation campaigns."[8] These actions have helped bring the United States and the European Union closer together as partners fighting the influence of non-market economies such

---

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/?.

[4] https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/?.

[5] https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/?("We intend to continue coordinating on our shared concerns, including ongoing human rights violations in Xinjiang and Tibet; the erosion of autonomy and democratic processes in Hong Kong; economic coercion; disinformation campaigns; and regional security issues. We remain seriously concerned about the situation in the East and South China Seas and strongly oppose any unilateral attempts to change the status quo and increase tensions. We reaffirm the critical importance of respecting international law, in particular the UN Convention on the Law of the Sea (UNCLOS) noting its provisions setting forth the lawful maritime entitlements of States, on maritime delimitation, on the sovereign rights and jurisdictions of States, on the obligation to settle disputes by peaceful means, and on the freedom of navigation and overflight and other internationally lawful uses of the sea. We underscore the importance of peace and stability across the Taiwan Strait, and encourage the peaceful resolution of cross-Strait issues. We intend also to coordinate on our constructive engagement with China on issues such as climate change and non-proliferation, and on certain regional issues.").

[6] https://www.commerce.gov/news/press-releases/2024/04/us-eu-joint-statement-trade-and-technology-council.

[7] https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/05/u-s-eu-joint-statement-of-the-trade-and-technology-council-3/.

[8] https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/.

as China and governments seeking to spread digital authoritarian restrictions to speech online—such as Russia.

However, Working Group 10 has failed so far to realize its potential or fulfill the commitments sought by the two parties when the TTC was first conceived. In the May 2023 Joint Statement of the United States and EU, the two parties agreed: "Within the Global Trade Challenges Working Group, the United States and the European Union intend to exchange information on non-market policies and practices affecting digital trade, as well as **on our respective policies linked to risks stemming from digital firms from non-market economies**."[9] The United States, to this point, has not leveraged the TTC to address the EU policies that perpetuate risks in non-market economies, such as China. In particular, U.S. digital services providers are subject to regulations and policies in the EU that directly support or embolden systemic rivals such as China and harm the competitiveness of both American and European firms on the global stage. The harms of these laws—both in the disclosures and restrictions they mandate and the thresholds that appear to specifically target U.S. suppliers—have not been addressed through the TTC. The implications of these laws on emerging technologies—such as artificial intelligence (AI)—and their relevance to competition with Chinese firms have also not been explored.

In pursuit of maximizing the cooperation between the two parties, so far, the TTC has avoided contentious issues such as the Digital Markets Act, the AI Act, the Data Act, and the Digital Services Act. This has occurred to the detriment of the broader goals of partnership in addressing global trade challenges, the remit of WG10. CCIA urges USTR to turn the page on this weakness of the TTC and to instead use the venue as a means of identifying, and as appropriate, remedying discriminatory or overly-burdensome harms of the EU's digital regulations on terms that work for both the United States and the EU. Doing so will benefit not only the U.S. firms operating in the EU, but also the EU economy as a whole, which has been found through several reports to be lagging, due in part to its regulatory posture, in the development of digital products and services needed to compete on the global stage.

[9] https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/ (emphasis added).

II. The Working Group Should Focus on Impacts of EU Regulations on Global Technological Competitiveness

USTR should refocus the workflow of WG10 to center conversations around inadvertent benefits EU regulations pose to Chinese companies, both in Europe and around the world. This would align with the initial intent of the TTC that has so far failed to materialize. This change is necessary to ensure that the TTC addresses the genuine problems in the realm of trade and technology, especially as it relates to foreign jurisdictions of concern. In the initial TTC Inaugural Joint Statement's Statement on Global Trade Challenges, the two parties illustrated a commitment to:

> To the extent practicable or deemed desirable by both the United States and the European Union, consult or coordinate on the use and development of such domestic measures, with a view to increasing their effectiveness and mitigating collateral consequences for either the United States or the European Union from any such measure developed.[10]

So far, from industry's perspective, there have been insufficient examples from the TTC and this Working Group in particular of the parties addressing the collateral consequences from the EU's domestic measures, as the following sections explore.

A. Evaluating Results of Data and IP Sharing Requirements on Security, Competitiveness

Elements of the EU's Digital Markets Act (DMA) have the potential to undermine the security of the United States, the EU, and the firms targeted by the law—which are, almost exclusively, from the United States. The DMA imposed significant obligations and restrictions on companies that are based in democratic countries without tangibly including similar limitations on Chinese or Russian digital services providers, effectively granting authoritarian rivals a direct advantage within the European market.[11] Although ByteDance is in scope of the

[10] https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/?.

[11] Obligations under the DMA include 1) requiring platforms to share proprietary first-party and third-party data, including data belonging to the U.S. and EU customers of platforms, and trade secrets that will enable rivals and malicious actors to exploit this data and undermine the security and safety of platforms; 2) requiring platforms to grant malicious actors direct access to core technical and operational infrastructure – including operating systems, hardware, and software tools – that are used to secure and protect digital services and technologies from foreign threats; and 3) deprive platforms of any meaningful opportunity to raise concerns or provide affirmative defenses in areas where compliance with a DMA obligation would undermine other values or principles relating to security, privacy, and intellectual property.

law for some of the DMA's requirements, there are no indications that other major technology competitors in China or Russia—such as Alibaba, Tencent, Huawei, Baidu, and Yandex—will be subject to oversight or obstacles under the DMA. None of these Chinese and Russian firms will need to comply with the DMA's strict rules, but they are all potential beneficiaries of the DMA in terms of their ability to gain preferential regulatory treatments (e.g., an unconstrained ability to engage in self-preferencing) and access to data and IP from U.S. firms.

The DMA could result in the forced transfer and disclosure of intellectual property, trade secrets, and sensitive business and user data to state-sponsored Chinese and Russian companies, through obligations to disclose data under 6.1(h), (i), and (j). These requirements could result in the sharing of l sensitive European data from both users and businesses—as well as trade secrets—to foreign rivals and bad actors that could potentially misuse that data to further their own interests. And as the European Data Protection Board recognized in Nov. 2021,[12] such transfers would take place without any consultation with DPAs or other competent authorities to assess the potential harms related to security and privacy.

One concrete example of the DMA actively benefiting companies from undemocratic countries is the requirement for gatekeepers to open their platforms to competitors. This led to Android being required to offer Yandex as a search option on the welcome screen due to the browser choice mandate, despite the browser consistently sending user metadata to servers based in Russia, where it has also shared data and encryption keys with the government.[13] Although the purported goal of the DMA is to offer additional choice for consumers at various stages of the digital ecosystem, the requirements of the law offer several "opening up" requirements such as the browser choice mandate that amount to promoting rivals from countries such as China and Russia in key digital services sectors.

The risks associated with the DMA's requirements are directly pertinent to the purview of WG10 and USTR should center these threats in their discussions with European counterparts going forward. The unintended consequences of the DMA—and, too, the Digital Services Act (DSA)—could be the strengthening of China, Russia, and other future undemocratic regimes

[12] https://www.edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf.

[13] https://www.ft.com/content/c02083b5-8a0a-48e5-b850-831a3e6406bb; and https://www.zois-berlin.de/en/publications/zois-spotlight/the-sad-fate-of-yandex-from-independent-tech-startup-to-kremlin-propaganda-tool#:~:text=In%202019%2C%20Yandex%20confirmed%20that,for%20the%20query%20'Navalny'..

with government-influenced firms competing against U.S. and EU suppliers. As such, it directly falls under the category of "global trade challenges," defined as "challenges from non-market economic policies and practices" in the parties' initial outlining of the TTC's makeup.[14] The link between the EU's requirements and the potential damage to security are clear. As Ambassador Wolfgang Ischinger, chairman of the Munich Security Conference, has argued in the context of the DMA and DSA, these laws should be "examined from every angle to ensure that they do not create unintended loopholes and problematic knock-on effects, or even increase the attack surface for those seeking to undermine the integrity and value base of liberal societies."[15] Former Deputy Assistant Secretary of Defense Evelyn Farkas has also noted that the DMA and other new regulations "should be coordinated and support our shared national security objective: keeping Chinese and Russian actors from acquiring data they could use against U.S, European, and even their own citizens."[16] Further, as a former Assistant to the President for Homeland Security and Counterterrorism has highlighted:

> "It does not require a giant leap of imagination to see how increasing the access of foreign competitors in Beijing and Moscow to user data and U.S. intellectual property could pose a real risk to cybersecurity. Over the long-term, regulation that specifically targets top U.S. tech companies risks creating a vacuum that Chinese tech firms, not European ones, are strategically positioned to fill."[17]

As USTR examines these issues with the European Union, it need not take the position that centering associated security risks necessarily means it is advocating for the reversal of the DMA. Including the DMA and related security risks for companies and governments alike instead means collectively seeking assurances that the DMA is subject to a meaningful security impact assessment, that the DMA does not inadvertently leave large Chinese and Russian tech companies unregulated, and ensuring that disclosure and access obligations under the law are subject to meaningful IP and security safeguards. Rather, the United States and the EU should seek to articulate the appropriate safe harbor for firms to be able shield themselves from these adverse outcomes, and not be subject to liability under the DMA. Additionally, USTR should

[14] https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/?.

[15] https://www.politico.eu/article/security-proof-eu-future/.

[16] https://www.politico.com/news/agenda/2021/09/20/digital-markets-act-eu-china-us-512602.

[17] https://thehill.com/opinion/cybersecurity/575148-ceding-regulatory-power-to-europe-will-weaken-the-security-of-the-free/.

seek regulatory dialogue to ensure that policymakers and industry are able to identify and address these risks before the harms materialize.

B. Analyzing the Thresholds for Regulatory Scope in Context of Competition with Global Rivals

The fact that many of the EU's marquée pieces of legislation—the DMA, the DSA, the DATA Act, and other subsequent laws—include thresholds for the strictest obligations and oversight that mainly, and in many cases almost exclusively include U.S. companies should be at the forefront of USTR's engagement with EU counterparts in WG10.

For rules that are facially neutral in application with respect to nationality, regulators should make transparent the process and standards for identifying who is and who is not in scope of regulation. Regulators should also ensure that these standards are based on meaningful assessments of risk and harm, where user base, revenues, and/or capitalization is demonstrably linked to harms, as opposed to being simply arbitrary thresholds. An emerging trend is setting thresholds for regulations to only apply to a subset of companies operating in the digital space (e.g., the "gatekeeper" concept in the Digital Markets Act and the "VLOP" concept in the Digital Services Act), and then using those thresholds as a proxy for risk and harm in a wide range of other regulations. Such thresholds may be both over- and under-inclusive in certain respects, and may result in vastly differential regulatory standards for similar types of activity.

These thresholds generally disproportionately target U.S. companies while allowing companies from third-party countries—including non-market economies—to operate outside the enhanced regulations imposed on firms that meet the threshold. This is particularly true of the DMA, where many other competitors to U.S. companies from China and Russia do not meet the thresholds (with the exception being ByteDance). Companies not captured under the DMA include Yandex, Tencent, Alibaba, Baidu, Temu, and Shein.

Further, these discriminatory scoping practices have been adopted by governments in key markets around the world where U.S. and European companies also compete against Chinese and Russian companies. The "gatekeeper" concept has been adopted in regulations that have

been adopted and still developing in South Korea,[18] Japan,[19] Turkey,[20] Saudi Arabia,[21] and Taiwan[22] for both competition and consumer protection policy. The spread of this idea and its application in these various contexts ensures that the harms of the policy, the security flaws it opens up, and the benefits it provides to rivals from China and Russia compounds and multiplies. This is particularly true as it is lifted to regions where these companies are already more competitive than they are in the EU. The TTC should offer exactly the sort of venue where the United States and the EU act as partners to ensure non-market economies and undemocratic societies are unable to undermine the growth of U.S. and EU digital export competitiveness.

III. The Working Group Should Focus on Strengthening Cooperation in Artificial Intelligence Technologies and Systems

To further progress in developing the TTC's AI Roadmap, the TTC should offer a forum for the United States and the EU to strengthen collaboration on artificial intelligence (AI) technologies and systems. This means both addressing the harms of premature and overreaching regulations that may follow from the *AI Act*, and proactively seeking regimes that facilitate cooperation in certification and standards to streamline cross-border trade. This work is firmly in line with the goals of the TTC as stated by the two parties—in the initial set of commitments between the United States and the European Union, the two committed to:

> The United States and the European Union recognize and respect the importance of regulation of goods and services to achieve legitimate policy objectives. They are also aware that such regulations may have unintended consequences and result in barriers to trade between them and that such barriers, once implemented, can be challenging to remove. **Consequently, the United States and the European Union intend to work to identify and avoid potential new unnecessary barriers to trade in products or services derived from new and emerging tech, while ensuring that legitimate regulatory objectives are achieved.**[23]

---

[18] https://ccianet.org/news/2024/09/ccia-responds-to-korea-fair-trade-commissions-shift-from-dma-like-policy-and-toward-new-regulatory-proposal/.

[19] https://ccianet.org/wp-content/uploads/2024/09/CCIA-Comments-in-Response-to-the-Japan-Fair-Trade-Commissions-Request-for-Information-Regarding-the-Japan-Smartphone-Competition-Act.pdf.

[20] https://ccianet.org/wp-content/uploads/2022/11/CCIA-Comments-on-the-Draft-Amendment-to-Law-No.-4054-of-the-Protection-of-Competition-in-Turkey..pdf.

[21] https://ccianet.org/wp-content/uploads/2022/11/CCIA-Comments-on-the-Saudi-Arabian-CITCs-Draft-Competition-Regulations-for-Digital-Content-Platforms.-PDF.pdf.

[22] https://english.ey.gov.tw/Page/61BF20C3E89B856/075117fd-6122-4f0e-bb38-a658306d6c59.

[23] https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/? (emphasis added).

A. The TTC Should Serve as a Venue to Address Harms of the EU's AI Act

The United States should pursue the TTC as a means of addressing the potential harms stemming from the EU's AI Act. The European Union sees the AI Act as an opportunity to set global norms: like GDPR, the AI Act is a first-of-its-kind regulation, with the potential to carry soft influence worldwide as businesses adapt to EU-specific requirements, and to inspire AI regulation in other regions, which brings it firmly within the ambit of WG10.

The AI Act definition of "AI system" aligns with the OECD definition. These systems are regulated by risk level: (1) low-risk systems are subject to transparency rules; (2) high-risk systems must comply with a comprehensive regulatory regime including numerous requirements such as conformity assessments, auditing requirements, and post-market monitoring; and (3) prohibited systems pose unacceptable risk and are banned. Specific rules introduced late in the legislative process will apply to providers of general-purpose AI models, with more stringent rules applying to models with systemic risks. The law will apply to both providers and users of AI systems where the "output" of that system is used in the EU. Fines for non-compliance can reach up to 7% of annual global turnover.

However, there remain several unclear definitions of AI systems, general-purpose AI models, classification of high-risk and prohibited AI, and allocation of responsibilities for actions in the AI value chain could lead to harms for firms from both the U.S. and EU. The broad definition of so-called "high-risk" applications, cumbersome compliance requirements and steep fines, create new compliance burdens for U.S. companies doing business in the EU. Additionally, the vague wording of certain prohibited systems creates legal uncertainty and risks banning low risk applications—the result of which has been many AI applications being unavailable in Europe despite successful launches elsewhere. Further, the expansive definition of "high-risk" in the AI Act could dampen innovations and create legal uncertainty and new hindrances for the pre-approval processes for products and services that are already subject to a multitude of regulatory mandates. Compliance requirements for "high risk AI" are administratively cumbersome and may not be technically possible for firms to adhere to with certainty, given obligations such as requiring human oversight and imposing responsibility in an opaque manner between AI developers ("providers") and deployers ("users").

The proportionate and flexible implementation of the AI Act's requirements, as well alignment with emerging international best practice and consensus, international technical

standards, will be key to providing providers and deployers of AI sufficient legal certainty to market AI systems and products in the EU. There are several areas in the AI Act's Code of Practice for providers of general-purpose AI models with specific need for engagement.[24] Further areas for cooperation in this area are covered in the following section.

B. The United States and EU Should Lay the Groundwork for Mutual Recognition Agreements for Conformity Assessment of AI Systems and Applications Through the TTC

Mutual Recognition Agreements (MRAs) for conformity assessments (where the latter is required under the AI Act)[25] can serve as a very useful method to boost cross-border flow of products and services. The ability for providers in one jurisdiction to be certified as meeting standards in their host country and have those outcomes acknowledged as sufficient in the target market reduces compliance costs and ensures cooperation in standardization policies. The United States and the EU have a strong history of MRAs in the telecommunications sector. As the National Institute of Standards and Technology has stated, MRAs can:

- "Reduce the time and cost of placing U.S. telecom products in foreign markets by eliminating the need for redundant testing and/or certification";
- "Encourage communications and information sharing among key stakeholders, including manufacturers, testing laboratories, certification bodies, regulatory authorities, designating authorities, and accreditation bodies"; and
- "Improve the transparency of foreign EMC and telecom regulations, laws, policies, and procedures, enabling U.S. manufacturers, testing laboratories, and certification bodies to more easily stay current on foreign regulatory requirements."[26]

The United States should seek to use the TTC to "avoid potential new unnecessary barriers to trade in products or services derived from new and emerging tech,"[27] through MRAs for conformity assessment. Having mutual recognition of what constitutes as safe or secure AI would enable U.S. and EU services and goods providers that rely on AI technologies to trade between the two jurisdictions, alleviating the possible barriers erected through either the AI Act

[24] https://ccianet.org/library/aia-code-practice-opportunities-challenges/.
[25] https://artificialintelligenceact.eu/article/43/.
[26] https://www.nist.gov/standardsgov/mutual-recognition-agreements-conformity-assessment-telecommunications-equipment.
[27] https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/.

or other developing laws and regulations in both the United States and the EU. The two parties have already acknowledged the importance of doing so in this space. Following a series of Dec. 2022 TTC meetings, the White House released a statement stating that the United States and European Union "recognize the importance of mutual recognition agreements and conformity assessment-related initiatives for U.S. and EU stakeholders engaged in transatlantic trade in a range of sectors" and committed to "explor[ing] ways in which the increased use of digital technology, where permissible, may help U.S. and EU stakeholders better utilize existing mutual recognition agreements to facilitate increased transatlantic trade."[28] CCIA urges the United States to continue pressing the EU to negotiate over pro-trade MRAs through the TTC, including to align with relevant ongoing processes in forums such as the Organization for Economic Cooperation and Development, the G7, and the G20.

IV. The EU's Current Regulatory Stance Harms Both American and European Economic Interests

The United States should use the TTC to reiterate the importance of maintaining a balance between consumer and market protection and pro-growth policies when approaching developing regulations. The results of the European Commission's regulations—lower productivity and innovation—have been highlighted recently in reports from Mario Draghi[29] and Enrico Letta.[30] As the Draghi Report highlights: "Regulatory barriers constrain growth in several ways… The EU's regulatory stance towards tech companies hampers innovation: the EU now has around 100 tech-focused laws and over 270 regulators active in digital networks across all Member States."[31] The TTC, particularly Working Group 10, is well-positioned to host discussions of regulatory shifts that would make Europe more competitive on the global stage against non-market economies, while also helping U.S. companies retain their edge over Chinese rivals.

The issue of addressing the vast regulatory burdens in the EU is not merely a matter of empowering the United States and EU to grow in internet services and productivity. It is also

[28] https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/u-s-eu-joint-statement-of-the-trade-and-technology-council/.

[29] https://commission.europa.eu/document/97e481fd-2dc3-412d-be4c-f152a8232961_en.

[30] https://video.consilium.europa.eu/event/en/27430.

[31] https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf at 28.

directly pertinent to WG10's goals. As Draghi argues, "limitations on data storing and processing create high compliance costs and hinder the creation of large, integrated data sets for training AI models," which results in "fragmentation [that] puts EU companies at a disadvantage relative to the US, which relies on the private sector to build vast data sets, and China, which can leverage its central institutions for data aggregation."[32] To ensure that the United States and the EU are able to compete with non-market economies like China, it will take both parties empowering one another to grow in key areas such as digital services. As such, the barriers to operation in the EU following years of overreaching regulatory frameworks are directly pertinent to the cooperation sought in WG10 and should be central to conversations between the two parties.

V. Conclusion

CCIA appreciates USTR seeking feedback on the future of the TTC and the Global Trade Challenges Working Group, and believes that the TTC can still serve as an effective forum for addressing trade disputes and global competition in digital services. For the venue of WG10, and the TTC overall, to fulfill its potential and successfully combat global challenges to trade—such as non-market economies like China—USTR should re-center the focus of collaborative work to address the EU's regulatory regime.

Respectfully submitted,

Amir Nasr
Trade Policy Manager
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
anasr@ccianet.org

Oct. 21, 2024

[32] *Id.*