Discussion Paper: How the EU-U.S. Trade and Technology Council Cooperation Can Navigate Conflict and Find Meaningful Cooperation on Data Governance and Technology Platforms

By: Nigel Cory

The first U.S.-EU Trade and Technology Council (TTC) meeting in Pittsburgh shows it is off to a good start, but that was the easiest part. The hard work lies ahead. The post-summit joint statement lays out the roadmap for each of the ten working groups (WG) to advance before TTC principals reconvene again in the spring of 2022. What matters is how the United States and the European Commission (EC) bring the roadmap to life by making progress on these and other related issues. In doing so, both sides will need to show that they're willing to compromise where they can and step out of their comfort zone where they must on new issues and forms of cooperation. Looming over deliberations is the skepticism based on recent bilateral turmoil and previous efforts at building transatlantic cooperation efforts which started with grand visions of cooperation but ran into the reality of varying expectations. Action and progress, especially on managing transatlantic data flows, will be key to success.

ITIF's report "How to Build Back Better the Transatlantic Data Relationship" details what's at stake. Negotiations for a new Privacy Shield agreement are focusing on how to remedy one of the principal defects identified by the Court of Justice of the European Union (CJEU)—a lack of independent oversight and redress in the U.S. system for Europeans who suspect the National Security Agency surveilled them. The outcome will likely be administrative (not legislative)—a non-executive U.S. agency such as the Privacy and Civil Liberties Oversight Board acting in combination with the Foreign Intelligence Surveillance Court (similar to U.S. administrative law judges). A key question is whether this solution is permanent enough (and thus defendable in the CJEU). U.S. officials telling firms to stay in Privacy Shield is hopefully a sign that a deal is almost done.

While the TTC has said it will not address Privacy Shield issues, there are a host of other key technology and data issues. TTC WG5 on data governance and technology platforms "is tasked to exchange information on our respective approaches to data governance and technology platform governance, seeking consistency and interoperability where feasible." Shared concerns include illegal and harmful content and their algorithmic amplification. Other issues are platform transparency, responsibility, and policies relating to sharing data with researchers and disinformation, product safety, and counterfeit products. It also notes an intention to share information on existing and future regulatory approaches and points to a shared interest in voluntary and multi-stakeholder initiatives on these issues. Cloud infrastructure may be discussed in this and other workgroups. Data and digital issues also cut across other working groups and issues.

The numerous references in the joint statement that both sides "should respect the different legal systems in both jurisdictions" should dispel any expectation that the United States would simply accept EU regulations and base discussions on data privacy, AI, and platform regulation around them. It would not be in the U.S. interest to harmonize regulations with the EU, nor is it necessary. There is no reason why there should not be different U.S. and EU regimes for most digital issues, as long as they are broadly aligned. Regulations don't need to be carbon copies to have a broadly similar effect. After all, Europe and the United States are unlikely to agree on a privacy framework or how to regulate AI. This is not to say that the two sides should not work toward common principles and regulations, but they should not expect to achieve complete convergence.

As to data governance, the two sides could explore (once a successor to Privacy Shield is enacted) the development of other data transfer mechanisms under GDPR, such as codes of conduct and certification schemes. These would provide a broader, flexible set of legal tools for firms from different sectors to manage data reasonably and responsibly under GDPR. Europe has been considering potential codes of conduct for the market research, health research, and clinical research services sectors. EU and U.S. stakeholders could work together to develop these. This would be based on the premise that Europe would not create "European data spaces" that U.S. researchers couldn't access. One specific idea is a certification or research framework for health and genomic data sharing for EU and U.S. researchers. COVID provided the lesson that discriminatory research access and restrictions on health data transfers are bad for public health.

Anti-trust and competition regulation is likely to be an exceptionally touchy issue given European regulators targeting U.S. firms. Europe is not only looking to use traditional anti-trust and competition policies, but also new approaches to regulating big platforms (the so called "gatekeepers"). This new approach is essentially a shift from ex-post judicial enforcement of antitrust rules to ex-ante regulatory rules. The DMA therefore illustrates a "precautionary antitrust." The EC's Digital Markets Act (DMA) and, to a lower extent, the Digital Services Act (DSA) outline a new set of competition policies that seek to reduce the power of big platforms. However, the prospect for alterations of the DMA or the DSA as part of transatlantic discussions is unlikely since Vice-President Vestager made clear that both are outside the scope of the discussions. This begs the questions as per the effectiveness and the remit of the transatlantic discussions with respect to the regulation of online platforms. One potential outcome is the proposed U.S.-EU Joint Technology Competition Policy Dialogue, which would focus on approaches to competition policy and enforcement. In line with this, Commissioner Reynders wants to be able to share information with the U.S. Federal Trade Commission, Justice Department, and Consumer Financial Protection Bureau about how those agencies can use the tools at their disposal to better protect consumers online. He also proposed restarting negotiations to update the EU-US agreement to cooperate on consumer protection.

On AI, the statement acknowledged their roles as founding members of the Global Partnership on AI (GPAI)—a multi-stakeholder group launched by the G7 to focus on the responsible development of trustworthy AI—both the United States and the EU agreed "to develop a mutual understanding on the principles underlining trustworthy and responsible AI." They committed to ensuring a policy environment that supports the deployment of trustworthy AI systems, cooperating across borders and sectors on responsible AI, and facilitating public and private investment in R&D to support trustworthy AI.

The TTC acknowledged that both sides have agreed that "policy and regulatory measures should be based on, and proportionate to, the risks posed by the different uses of AI." However, each side has a very different approach to achieving that goal. The EU has proposed legislation, the AI Act, which would subject high-risk uses of AI to certain (onerous) requirements, whereas the United States has proposed a voluntary risk management framework to guide the development and use of AI systems. As long as the EU does not attempt to impose their restrictive AI Act regulations on U.S. companies doing business in the U.S., such a divergent regulatory framework should not be problematic. However, the two sides could find specific issues to work together on such as sectoral areas for AI cooperation, including in autonomous vehicles, financial trading, etc.

As to cooperation on platform issues, a significant potential area for collaboration is the issue of providing greater access for researchers to access platform data. But a key barrier to overcome is the legitimate concerns from platforms (particularly social media) that want to make sure they aren't violating any laws (especially privacy) in sharing data. They also want to make sure researchers adhere to their terms. So there's an opportunity for the United States and EU to work with industry to develop a code of practice around research access to platform data (around various issues, including social media, online fraud, etc.).

There is also an opportunity for pragmatic cooperation on platform policies to counter counterfeit products. "Know your business customer" policy is central to preventing bad actors from operating under a cloak of anonymity. But the key issue is how best to identify them. The EC is considering several proposals. It'd be great if these were added to the Digital Services Act (DSA). The United States is considering minimum requirements for online platforms in the SHOP SAFE Act and INFORM Consumers Act. Given the alignment of timing and interest, ideally, rather than have the DSA set up one set of rules and the United States pursue a different set, the two sides could harmonize rules based on industry best practices.

TTC principals stressed the need for transparency and stakeholder engagement. The Department of Commerce, State Department, USTR, and European Commission have launched websites and public consultations on the TTC. It's incumbent upon those that want the TTC to succeed to engage and put forward helpful research and pragmatic proposals.

Some of ITIF's ideas. First, a U.S.-EU quantum computing agreement. The United States has recently concluded agreements with Japan and the United Kingdom on quantum computing policy, which contrasts with early proposals in Europe to preclude such cooperation with the United States. Second, both sides could explicitly exclude U.S. and EU investments into defense technology investments from the review process (as proposed by the National Security Commission on AI). This would support greater cooperation on AI for defense-related purposes. Third, the TTC's work on AI measurement is a good idea, but they could do more. For example, the two sides could develop shared, representative datasets of faces to serve as a more reliable resource for organizations developing facial recognition technology. Fourth, the two sides could work together on pre-standardization cooperation on new and emerging technologies. Such cooperation (already used for advanced materials and nanotechnology) brings respective agencies together early to develop standardized terminology, reference materials, and testing and measurement protocols for new materials (physical, chemical, material, electronics etc.)

Europe and the United States have more in common than they tend to admit—even when it involves contentious issues—and their shared values stand in stark contrast to those of authoritarian digital powers such as China and Russia. It's essential EU and U.S. policymakers realize the enormous economic and innovation stakes involved as they consider the next steps for the TTC. Weakening transatlantic digital engagement and cooperation will accelerate the fragmenting of the global digital economy as it'd reflect a fundamental fracture between two key players. Such a scenario would hurt Europe and the United States by a lot more than what's directly at stake in the transatlantic digital relationship (which is already significant). To avert this costly scenario, both sides need to focus on delivering concrete results in 2022. In doing so, they would set the foundation for broader cooperation on digital and technology issues at the United Nations, G7, WTO, and elsewhere.