# Transatlantic Dialogue on Reawakening Digital Trade: Parts I and II – a Summary

***Since 2019, the transatlantic dialogue constitutes a joint format for discussion on digitalization topics of high relevance to both the U.S. and the EU, introduced by the European-based eco – Association of the Internet Industry (eco Association) and the U.S.-based Internet Infrastructure Coalition (i2Coalition). The two latest transatlantic dialogues were held in Washington, D.C. and Brussels to discuss the details of the future of the Trans-Atlantic Data Privacy Framework.***

## **Part I:** Diverse Stakeholder Considerations Around the Future of the Trans-Atlantic Data Privacy Framework

The Part I roundtable discussion took place on 6 October 2022 in Washington, D.C., the day before President Biden signed a new Executive Order on Enhancing Safeguards for United States Intelligence Activities. The dialogue was co-hosted by **Christian Dawson**, Executive Director of the i2Coalition and **Oliver Süme**, Chair of the eco Association Board and Partner at Fieldfisher. The distinguished panel speakers included **Ruth Berry**, Acting Deputy Assistant Secretary for International Information and Communications Policy, Bureau of Cyberspace and Digital Policy at the U.S Department of State; **Kate Charlet**, Director for Data Governance, Google; **David Snead,** General Counsel at cPanel & Co-Founder of i2Coalition; **Alissa Starzak**, Vice President, Global Head of Public Policy, Cloudflare; and **Catherine Stihler**, CEO, Creative Commons.

### Part I: Lightning Talk

**Ruth Berry** commenced her lightning talk by reporting that, on 25 March 2022, U.S. President Biden and EU Commission President von der Leyen had announced a deal in principle on a new Trans-Atlantic Data Privacy Framework. Over the prior eighteen months, Berry herself had been heavily involved in the intensive negotiations. Since then, the U.S. had been working to translate the deal in principle into legal language that would be released in the form of an Executive Order and Department of Justice regulations. Berry was of the opinion that this deal would address the deficiencies of the previous Privacy Shield Framework, as outlined by the Court of Justice of the European Union (CJEU) in the Schrems II decision, and that the deal would provide a durable basis for transatlantic data flows that are critical for underpinning the $7.1 trillion transatlantic economy.

The new deal was viewed by Berry as putting in place rigorous protections regarding the necessity and proportionality of signals intelligence collection, and creating a multilayered, binding, and independent redress mechanism for those who feel that their data has been improperly accessed by U.S. intelligence or law enforcement.

As a representative from the U.S. Department of State, Berry highlighted the fact that she comes from the new Bureau of Cyberspace and Digital Policy, with this bureau bringing into one unit work on international security and cyberspace, as well as work on international communications, information policy, and digital economy. She also described a new digital freedom unit within the bureau, which is seen to enable the department to both integrate the national security, human rights, and economic issues when it comes to digital and emerging technologies. Key issues being dealt with by the bureau include data policy and data privacy, data governance, and data sovereignty. The bureau seeks to work with a community of like-minded democracies in developing

shared approaches to these challenges, that reflect a strong commitment to privacy protections while simultaneously allowing cross-border data flows that open market-led economies and societies, with the new Trans-Atlantic Data Privacy Framework representing this commitment. From Berry's perspective, having the U.S. and the EU working together on these issues is creating strong opportunities for both sides to turn globally and think about how they are working to help build a 21st century future that embodies these democratic principles. Berry also introduced two other particularly important efforts in this space. These include, firstly, the bureau's work with the partners and allies at the OECD in developing shared high-level principles on trusted government access to data held by the private sector and, secondly, the globalization of the cross-border data privacy rules systems.

After the eighteen months of negotiation in which the bureau was involved, Berry expressed her confidence that the deal fully addresses the CJEU's concerns and will stand as a durable solution. While she nonetheless anticipated a future legal challenge, her view was that there is a lot more commonality than a differentiation between the U.S. and the EU counterparts and that the durability of the solution would be supported by taking on board the work of the European Member States. When it comes to the current reforms, as she sees the U.S. to be in good company among its European allies, she believes that this should help to put both parties on firm footing when it comes to the CJEU's reviews.

## Part I: Inputs from the Panel Speakers

Each one of the panel participants commended the U.S. and the EU on the work that had been undertaken to achieve the deal in principle and to release the Executive Order. From the civil society perspective, **Catherine Stihler** welcomed what she saw as a positive outcome from the intense eighteen-month discussions on the new framework. On her part, **Kate Charlet** regarded this deal as particularly important, given that people would like to be able to access digital services from anywhere in the world, while simultaneously wanting to have their information kept safe and protected. Charlet proceeded to report that Google has long advocated for reasonable limits on government surveillance, and thus welcomed the fact that the U.S. is committed to enabling independent and meaningful redress for people in the EU, to strengthen the guardrails and proportionality around U.S. intelligence collection, and to ensure effective oversight over these new privacy and civil liberties standards. Chartlet also commented that the U.S.-EU data flows discussion demonstrated how there needs to geopolitical level trust between all countries where data is flowing. In her endorsement of the deal, **Alissa Starzak** homed in on the valuable shared vision of privacy. As she pointed out, until now, in the EU there had not just been issues concerning legal uncertainty, but also the perception from a company standpoint that the U.S. and the EU were not aligned on privacy. Starzak visualized that the shared vision apparent from the deal would improve long-term help for U.S. companies, including SMEs, and enable cross-border work. Starzak also emphasized that data flows are not only key for business and transatlantic economy, but also for cybersecurity and for resilience. Finally, **David Snead** noted that having something that is easily implementable helps consumers, given that it will lead to compliance with the GDPR.

From his end, in contemplating the deal in principle, **Oliver Süme** indicated his conviction that it could not only stimulate the economy, but could also serve to end the huge legal uncertainty that European businesses, and in particular the SMEs, are currently facing. In the past, the Privacy Shield was regarded as the most important legal ground for international data transfer, in particular for SMEs. At present, while many businesses are currently working with standard contractual clauses, these are regarded as quite challenging for implementation in a proper and compliant manner. As such, the core benefit of the new framework (as was the case with the prior Privacy Shield) was identified by Süme as the fact that data flows should be much easier to handle. Under the old Privacy Shield, he noted that there was simply a need to register in an easy and

comfortable manner, meaning that SMEs could rely on a very stable and easy legal ground under the GDPR for international data transfer. Süme's expressed hope was that this would again be the case in the future, which should not only stop the situation of legal uncertainty, but which would also stimulate data transfer and a global data economy on both sides of the Atlantic.

Süme also speculated on the timeline for the further process of the framework, pointing out that, from the European administration perspective, consultations would need to take place with the European Data Protection Board and European Parliament, and the administration would subsequently have to publish the whole agreement in their gazette. This would lead to a minimum of a three-to-four month follow-up to the deal in principle. The data protection watchdogs would also need to find a position for this situation, and, most importantly, would need to align with the European data protection authorities.

In closing, a number of the panelists discussed the topic of the language of the framework. **David Snead** remarked that, while "legalese langauge" (that is, the specialized language of the legal profession) is important, it is also essential that it is understandable for European consumers in order for them to know that they can restrain U.S. surveillance issues, which are a continual problem for the adoption of U.S. technology in Europe. On a similar note, **Kate Charlet** and **Alissa Starzak** commented that the Executive Order and the surveillance changes need to be well explained, clear and actionable, but that they also need to involve legalese language, insofar as the framework involves legally binding instruments that are subject to scrutiny and review. Luckily, as **Catherine Stihler** noted, there have been significant advances in ensuring that legalese language is more and more available in very plain English, particularly on the consumer protection level.

## **Part II:** The Future of the Trans-Atlantic Data Privacy Framework

On 6 December 2022, the Part II roundtable discussion was held in Brussels. This dialogue was moderated by **Lars Steffen**, Director International at the eco Association, and co-hosted by **Alexander Rabe**, Managing Director of the eco Association, and **David Snead**, General Counsel at cPanel & Co-Founder of i2Coalition. A lightning talk was provided by **Geneviève Tuts**, Head of Cabinet at the European Commission Directorate-General for Justice and Consumers (DG JUST), while the two additional panel speakers were **Iverna McGowan**, Director at the Europe Office of Center for Democracy and Technology¸ and **Corinna Schulze**, Senior Director at EU Government Affairs at SAP.

### Part II: Lightning Talk

**Genevieve Tuts** is Head of Cabinet of the EU Commissioner for Justice, Didier Reynders, who is the chief EU negotiator on the Trans-Atlantic Data Privacy Framework. Based on her personal experience in the negotiations, at the Part II roundtable discussion Tuts noted that a very detailed discussion with the U.S. counterparts had taken place, allowing a common understanding to be reached and complex issues to be resolved, with this resulting in a delicate balance between privacy rights and national security needs.

In providing a background to the framework, Tuts reported that, on 7 October 2022, President Biden signed a new "Executive Order on Enhancing Safeguards for United States Intelligence Activities" (hereinafter referred to as the "Executive Order"), with this order emerging as the outcome of intense discussions that had commenced in March 2021. The Executive Order was complemented by a Regulation adopted the same day by the U.S. Attorney General Merrick Garland. As Tuts noted, these two announcements can be viewed as an extremely important step

towards developing the new Trans-Atlantic Data Privacy Framework after the invalidation by the Court of Justice of the European Union (CJEU) in the "Schrems II" decision. In this context, safeguards contained in the Executive Order address the concerns raised by the CJEU and bring significant improvements vis-á-vis the comparative Privacy Shield. In short, the Executive Order deals with two aspects:

1) New binding safeguards;
2) A completely new redress mechanism with the Data Protection Review Court (DPRC).

With regard to the binding safeguards, Tuts described these as involving new rules that regulate under which conditions U.S. intelligence agencies can collect and use personal data transferred from the EU to the U.S. These rules are binding for all American intelligence agencies and ensure that any access to data will be limited to what is necessary and proportionate to protect national security. One of the core aspects of the Executive Order concerns the legitimate objectives that can justify data collection and that lay down detailed conditions for the collection, use and sharing of data.

Regarding the redress mechanism of the Executive Order, Tuts spelt out that any European will be able to lodge a complaint via this mechanism free-of-charge, and can access this mechanism if they consider that the personal data was unlawfully assessed by a U.S. intelligence agency. The new mechanism has two different parts: Firstly, it's independent and has a binding authority, which is the so-called Civil Liberties Protection Officer (CLPO) in the Office of the Director of National Intelligence (ODNI). Complainants will enter that initial investigation to determine if the safeguards or other laws have been violated and, if so, determine the appropriate remediation. Secondly, when it comes to the DPRC, individuals will have the possibility to appeal the decision and the DPRC will have the power to investigate such complaints and issue binding decisions. This Court will be composed of judges chosen from outside the government, who will be appointed on the basis of specific qualifications and will therefore allow for the independence of these courts.

As Tuts indicated, there is still some work to be done to fully implement the safeguards in the U.S., with the U.S. intelligence agencies, for example, having to implement the Executive Order in their internal policies and procedures. This might take up to one year.

In turning to the EU side, Tuts described how the Commission is currently preparing the draft adequacy decision based on the Regulation and the Executive Order. In launching the process towards the adoption of the adequacy decision, a number of different steps will follow, involving three requirements:

1) obtaining an opinion from the European Data Protection Board (EDPD);
2) receiving a positive vote from the Member States in a comitology procedure;
3) attaining input from the European Parliament.

Following these steps, the Commission will be able to adopt the adequacy decision, with Tuts' optimistic expectation being that the framework could be adopted in six months time. From that moment on, companies will be able to rely on this adequate transfer of data to the U.S.

In Tuts' final overview on the framework, she noted that, when the Commission negotiated this agreement, the question was always to have the right balance between private rights and national security needs. Tuts sees the balance to have been solidly achieved through two main elements:

1) the principles of proportionality and necessity; and
2) the safeguards which give citizens the possibility of an access to a real redress.

Ultimately, Tuts anticipates that the CJEU will determine if this balance is acceptable.

## Part II: Reviews from the Panel Speakers

In commencing her input, **Iverna McGowan** described how the Center for Democracy and Technology Europe Office (CDT Europe) is a not-for-profit organization focused on protecting democracy and international human rights law on a global level. With regard to the Trans-Atlantic Data Privacy Framework, CDT Europe is of the opinion that there have been some exceptional steps made with the new Executive Order, with one of its most profound factors regarded as the explicit reference to the principles of proportionality and necessity. As a legal tool extracted from international human rights law, this is a particular factor that CDT Europe is analyzing, based on the details of the Schrems II decision. As McGowan noted, in this decision, the CJEU recognized the overall national intelligence aims as being legitimate, but it did state in particular that Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 could not be regarded as strictly necessary, given that they adopted a more generalized approach to surveillance rather than a targeted approach. As the court stated, under EU law, a clear scope and precise rules governing the surveillance would be required. With regard to the present framework, CDT Europe still sees a risk that the twelve permissible objectives of surveillance could be determined as disproportionate: for example, because the short list of permissible surveillance objectives might not actually be narrow or precise enough according to what the court has ruled. As such, CDT Europe has recommended a need for clarification and greater assurance that the categories provide a meaningful limit to the scope of surveillance. In turning to the view of CDT Europe on the new redress mechanism, McGowan stated that this was considered to be of the utmost importance, given the prioritisation of this issue by the CJEU. Nonetheless, while the mechanism amounts to a ceding of authority of elements of the U.S. intelligence community to the CPLO and the DPRC, CDT Europe has concerns regarding the redress process, both due to a perceived room for improvement around the point of a fair hearing and representation, and the importance of the independence and impartiality of the decision-making body.

In presenting his perspective from the i2Coalition and U.S. angle, **David Snead** emphasized the need to advocate for U.S. surveillance reform, which he believes will make the Executive Order more durable, with settings such as reauthorization coming on board from Section 702 of FISA. As Snead stated, support from the EU in helping the U.S. with surveillance reform will be key to creating an adequate privacy regime in the U.S., in addition to helping the U.S. to support a federal privacy policy. In this context, it would be crucial for the EU to understand the U.S.'s particular surveillance needs and to appreciate that these are not unique to the U.S., but also take place in Europe.

Snead argued that elements are required to refine these activities, in order to make them less burdensome on companies who are processing data internationally, bearing in mind that the issue from Schrems II was not business access to data, but government access to data. In homing in on the potential for the U.S.'s federal privacy policy, Snead expressed his hope that this would be approved by the forthcoming Congress. Ideally, this would involve federal legislation that has state preemption; namely, a uniform privacy legislation across the U.S. Snead emphasized that, if the federal government does not step in with a uniform policy, it would be particularly onerous, given that various states are currently filling the void and implementing their own privacy legislation.

**Corinna Schulze** provided core insights from a company's perspective, emphasising that what was particularly important to bear in mind in discussions on data flows was the fact that all the data is not the same. As she pointed out, her business-to-business company processes a significant level of data on behalf of their customers and that, while legal certainty is important, it is even more important to appreciate the nuances of all data. As Schulze noted, the role of businesses is not to funnel data to governments, with this also not being desirable from the customer perspective.

While companies themselves require privacy policies that customers can rely on, any expectation to channel data to governments for surveillance runs a high risk of hindering the digital economy.

Nonetheless, while Schulze acknowledged that the overall data privacy process is cumbersome for companies, she welcomed the fact that all businesses have consequently become more mature in their consideration of data transfer. While the present Trans-Atlantic Data Privacy Framework involves the EU and the U.S., many companies naturally also need to bear in mind the repercussions of data transfer to other countries, particularly those that are not genuine democracies. As such, she would anticipate a valuable impact of the Privacy Framework on other international agreements. In conclusion, she added that, aside from the value of the Privacy Framework, an additional emphasis should be simultaneously placed on technical security measures.

From his end, **Alexander Rabe** noted how important initiatives such as Gaia-X were in protecting data and managing its safe and special transfer. Furthermore, he referred to the fact that, in opening the field of cybersecurity, it is also essential not to weaken the field of encryption. As Rabe also noted, data privacy should not be essentially observed as the showstopper for digital transformation. What is therefore potentially required – particularly with a possible forthcoming Schrems III court decision – is greater precision and clarification. All in all, Rabe held a very positive view on the potential for transatlantic data flows. In this respect, he referred to the EU's data economy's value between 2018 and 2025, which is projected to rise from approximately 301 billion Euro to 829 billion Euro.

**In closing, all of the speakers concurred that the compliance features of the Trans-Atlantic Data Privacy Framework offer a significant opportunity to stimulate digital businesses on both sides of the Atlantic, with the forthcoming six months offering a key opportunity to arrive at greater clarity and more precise rules.**