eco Association and i2Coalition – High-Level Transatlantic Dialogue on the EU-US Privacy Shield

Report on the Roundtable Dialogues in Brussels and Berlin

In an increasingly digital world, data is an invaluable resource and a key driver of innovation. However, to safeguard data sovereignty and informational self-determination, the use of data in the interest of all citizens must be reconciled with rights for effective protection of personal data. These were the opening words of Nadja Hirsch, Member of the European Parliament, at the first of two transatlantic roundtable discussions which took place on 7 and 12 February in Brussels and Berlin respectively.

The roundtables were jointly hosted by eco – Association of the Internet Industry and the US-based i2Coalition (Internet Infrastructure Coalition), and brought together representatives of the Internet industry from both sides of the Atlantic. These included Google, Dropbox, ICANN, EuroISPA, BEUC, Access Now, CENTR, TechGDPR, Verizon, Fraunhofer Institute, and the American Chamber of Commerce in Germany. Also in attendance were members of the EU Parliament, members of the German Bundestag, and representatives of other European bodies, such as the European Data Protection Board and Data Protection Authorities. The core focus of the dialogues was on the future of international data transfer between the EU and the US – and, in particular, on that of the EU-US Privacy Shield.

The EU-US Privacy Shield – An Overview

As Hirsch observed, while transatlantic data flows are indispensable to both the EU's and US's economies, data protection regimes in both regions differ substantially. This is where the EU-US Privacy Shield comes into play. As a successor to the earlier Safe Harbor Agreement, the EU Commission adopted the Privacy Shield with two objectives in mind: long-term legal certainty for companies, and a solid framework agreement to safeguard the protection of personal data, even in the light of different business models.

Hirsch holds the Privacy Shield to be a much better framework than the Safe Harbor and pointed to improvements in the areas of control, enforcement, transparency, and liability. She perceives the Shield as offering EU citizens more options to file complaints regarding data privacy and ensuring a higher level of documentation and monitoring of the compliant companies in both the US and the EU. Most importantly from Hirsch's perspective, an Ombudsperson mechanism has been created for the US to allow for individual redress and independent oversight.

However, as Hirsch argued, every protection regime is only as good as its application and enforcement. In the US, she believes that wide-ranging governmental access to personal data for security purposes undermines the protection of fundamental rights. Surveillance measures still do not require a proportionality assessment and the various redress procedures for EU citizens in the US may be too complex to use and therefore less effective. As Hirsch sees it, the introduction of an Ombudsperson was a step in the right direction, but this mechanism has yet to be implemented and there are still major questions concerning its independence and competences, especially vis-à-vis surveillance services.

Whereas the European Commission maintains that the Privacy Shield offers an adequate level of protection, last July, after much debate, the European Parliament finally called for a suspension of the

agreement. In this respect, Hirsch urges the Commission to exert more pressure in order to resolve the Privacy Shield's structural shortcomings.

Challenges to the EU-US Privacy Shield

Oliver Süme, Chair of the eco Association, moderated both the Brussels and Berlin roundtables. He emphasized the importance of this overall dialogue in light of the fact that the Privacy Shield – despite being one of the most important legal grounds for transferring data from the European Union to the US – is being challenged in Europe. Süme also referred to a second potential legal ground for a lawful international data transfer: the so-called Standard Contractual Clauses. But this construct is also coming in for criticism and is currently subject to a case brought by Max Schrems (a case referred to as "Schrems 2.0") to the European Court of Justice (ECJ). As Süme cautioned, were the Privacy Shield to be declared invalid and the Standard Contractual Clauses annulled, the practical implications for the greater part of the industry would be an overnight removal of grounds for lawful data transfer.

At the Berlin roundtable, Ronja Kemmer, Member of the German Parliament, stated that the Christian Democrats and Christian Socialist parties regard the Privacy Shield as crucial for economic ties between the US and Germany, as well as between the US and the EU. As such, Kemmer expressed her satisfaction at the positive outcome of the EU Commission's report on the topic from December 2018, which contends that the agreement provides an adequate level of data protection, and therefore provides a good basis upon which to build. Furthermore, while acknowledging its weak points, Kemmer echoed the view from the Brussels roundtable that the Privacy Shield, when compared to Safe Harbor, contains significant improvements, particularly with regards to standards and transparency. To keep it in place, it is crucial to address what Kemmer regards as its most prominent weakness: namely, the continued lack of appointment of an Ombudsperson in the US. Here, Kemmer underlined the importance of the EU's deadline for this appointment (which was scheduled for 28th February at the time of the roundtables; Keith Krach has been nominated for this position) and called for strong negotiations with the US for the full independence of this post. Kemmer also exhorted the German government to use its role as an intervener before the ECJ to support the Privacy Shield.

Insights from European Data Protection Representatives

The roundtables benefited from two detailed inputs from representatives of European data protection bodies. In Berlin, Peter Schaar – former German Federal Data Protection Officer and current Chair of the European Academy for Freedom of Information and Data Protection – traced the chronological evolution of the Privacy Shield and offered key insights into its current status. In Brussels, Willem Debeuckelaere, a Deputy of the European Data Protection Board (EDPB), likewise outlined the agreement's history and contributed important observations on the Shield.

As both specialists explained, the Privacy Shield, and the EU General Data Protection Regulation (GDPR), both have their origins in the Council of Europe's Convention 108 from 1981, and the subsequent 1995 Directive 95/46EC. As such, what is in focus when discussing the Shield and its future is a work in progress that has already been on the table for many decades. Debeuckelaere also emphasized that the Privacy Shield is a legal instrument based on Directive 95/46EC, meaning that the GDPR itself is not being questioned; in fact, the GDPR is likely to be the most important text for further negotiations and assessments of the Shield.

According to the two specialists, the main thinking of the European GDPR is that, outside of Europe, European data should be protected at approximately the same level as within Europe, albeit not

necessarily using the same instruments. The most important instrument for providing an adequate level of data protection for transferred data is Article 45 of the GDPR, that is: “Transfers on the basis of an adequacy decision”. This establishes that a non-EU country ensures an adequate level of protection of personal data by reason of its domestic law and international commitments. Debeuckelaere described this as an extension of sorts of the sphere of justice and data protection from the European side to other organizations or countries.

Other instruments that also can be used are: the standard contractual clauses; binding corporate rules (where a group of companies or a company which is active in different parts of the world approves a binding system, with the GDPR containing very specific requirements for BCRs); or a more exposed category of contractual clauses and informed consent.

In order to understand current deliberations, both specialists believe it is important to understand the history of the Privacy Shield’s predecessor. The Safe Harbor Agreement ultimately floundered in 2015, with its annulment having major ramifications for thousands of companies which based their data transfer on this system. It was declared invalid due to an ECJ judgment that ruled that an adequate level of protection was not being afforded to data by the US, due to the level of exemption applied by the US to state access. The ECJ concluded that the adequate level decision must take into account all relevant aspects, including government activities and law enforcement and intelligence, which effectively triggered a renegotiation and revision of the agreement. While “adequate level” does not necessarily mean that there should be identical legal instruments, ultimately an equivalent level of data protection must prevail.

In 2016, the Commission agreed on its new adequacy decision, the Privacy Shield, which according to the two speakers installed some improvements and additional safeguards. Paramount to these was the creation of the Ombudsperson mechanism in the US for the handling of complaints or enquiries raised by EU citizens, particularly with regard to US government access to data. The Ombudsperson is to act independently and be associated with the US Department of State. Significantly, the US Congress also adopted the Judicial Redress Act, which provides higher legal guarantees for non-US persons who are covered by data protection regulation. A further new and distinguishing factor of the Privacy Shield is its contingency on annual review.

Commenting on the differences and similarities between the Safe Harbor and the Privacy Shield, Schaar noted that the Privacy Shield has much the same structure as Safe Harbor, with its core instrument being the self-certification of companies. Rather than constituting an international treaty, it is therefore an intergovernmental agreement that can be repealed by the government. Schaar signaled that, in the execution of the Privacy Shield, ample room exists for improvement. Even today, after the adoption of the Judicial Redress Act, Schaar noted that there is no complete equality of EU citizens with US persons. While rights exist under the Act to turn to the Ombudsperson and ultimately the court, other procedures have first to be looked to. Furthermore, data of third-country nationals which are transferred based on the Safe Harbor are not subject to the safeguards. And perhaps most significantly, as in the previous agreement, national security remains exempted in the Privacy Shield.

Nonetheless, as Schaar reported, the two Privacy Shield annual reviews which have been conducted to date reveal improvements, in particular with regard to private sector data processing. Even in the field of access of US authorities to data, some progress was evident. On the other hand, some of the main points of concern still have to be resolved, as the EDPB has stated, particularly with regard to the national security exemption. Both Schaar and Debeuckelaere argued that the extent of the reach of this exemption must be made clearer, given that nobody can presently tell to what extent data will be used

by the NSA, CIA, etc. for their own investigations. Reauthorization of Section 702 of the US Foreign Intelligence Surveillance Act (FISA) has not provided additional safeguards, with Section 702 meaning that the NSA and other intelligence authorities, even the FBI, might be active against non-US persons; and one of the requirements of data protection regulation is to limit these powers. While the FISA was up for revision, this has been put on hold.

In the main, Debeuckelaere indicated a degree of concern felt by the European Data Protection Board concerning the commitment to the Privacy Shield, particularly in view of the lapse of two years since the inception of the Privacy Shield and yet the continuing absence of an Ombudsperson. Nonetheless, Debeuckelaere viewed with a level of optimism the shifts in the US in terms of some state law and companies' thinking. In Debeuckelaere's view, if the goal of tech companies to produce a federal law is attained, then the situation would improve substantially.

On his part, Schaar concluded that, while there are clearly still significant issues to be tackled, the documented levels of improvement offer room for optimism that the Shield will remain in force.

Key Insights from the US Internet Industry

David Snead, Policy Working Group Chair and Co-Founder of the i2Coalition, was a key speaker at both roundtables and provided valuable insights into the current situation and, crucially, the thinking in the US. Snead started by emphasizing that, contrary to widespread European opinion, privacy issues are extremely important on both sides of the Atlantic (indeed, as Willem Debeuckelaere reflected, the origins of the concept of "the right to privacy" hail from 1819 in the US). The tendency to underestimate the importance which privacy issues are warranted in the US can in part be attributed to differing cultural expectations concerning what needs to be kept private. In the US, for example, expectations of privacy originate from the fourth amendment and center on state surveillance, with no constitutional right to privacy in data given to companies. Snead also homed in on the differences between the US and EU political systems, emphasizing in particular the length of time it takes for rollout of legislation in the US.

Progress is nonetheless evident. As Snead recounted, there is an unprecedented level of activity currently occurring in the area of privacy, with at least seven bills on privacy alone being proposed in the US Congress, coming from both the Republican and Democrat aisles. These include a bill from the Center for Democracy and Technology, a privacy bill proposed by Intel, an executive branch action spearheaded by the National Telecommunications & Information Administration (part of the Department of Commerce), and a proposal for creating privacy standards emanating from the National Institute of Standards and Technology. In addition, there are a number of states that are considering privacy legislation; notably, California has recently passed privacy legislation that is largely modeled on the GDPR, while even the traditionally conservative state of Texas now has a biometric privacy legislation. As such, it's clear that things are moving.

Nonetheless, there are a number of questions that need to be answered in the US in terms of privacy legislation. The first is that most legislation that has been proposed would be enforced by the Federal Trade Commission (FTC) – and yet, the FTC may have insufficient authority under its charter to exercise that enforcement. The second concerns the fact that, while a number of US states are starting to pass their own privacy legislation, uniform privacy legislation in the US would require a uniform law. This is feeding into the current debate about whether federal legislation should pre-empt state legislation, a concept which, according to Snead, is particularly popular with the Speaker of the House. The third question concerns who the parties with responsibility for enforcing US privacy legislation will be – that

is, whether enforcement will be confined to regulatory enforcement, whether State Attorney Generals are also going to be able to enforce such legislation, and whether there will also be a private right of action. All in all, Snead reported that US citizens seem determined to find a way to have laws enforced.

With regard to the Ombudsperson mechanism, Snead stated that the new Ombudsperson has been nominated and his name sent to Senate, and that the appointment as such now seems to be relatively procedural. There is therefore an expectation that the current selected candidate will soon be confirmed, although whether this would happen by the deadline of 28th February was not clear at the time of the roundtables (Keith Krach has been nominated for this position).

In response to questions on the self-certification process in the US, Snead responded that it entails a very rigorous and indeed somewhat onerous process. Whilst there is no obligation on US companies to have a privacy policy, as soon as a company has such a policy, it becomes part of their customer contract, ushering in the right to action for any violations. However, in spite of its non-obligatory status and the challenges that it presents, Snead finds that companies are not necessarily resisting the Privacy Shield; rather, they are grappling with changing their business models to meet altered expectations about privacy. And, as it transpires, many companies in the US actually have a lot of experience of dealing with privacy, given that similar requirements exist under the health care privacy law, which also require companies to ensure supply chain compliance.

In terms of getting companies to adopt the Privacy Shield, Snead pointed out two important factors: The first is education, involving a shift in terms of how companies think of and handle data. The second is enforcement, meaning that the more lawsuits and the more economic impacts that non-compliance has, the quicker these companies will come into compliance.

Expanding on the theme of enforcement, Snead reported that the FTC is taking enforcement action against companies who infringe their Privacy Shield (or earlier Safe Harbor) obligations. While only a limited number of cases are pursued by the FTC each year (numbering just five in 2018), these are strategically chosen and rigorously pursued.

Effectively, in the US there are two paths of redress that can now be followed:

- the first being to approach a person/company's Data Protection Authority, who can in turn approach the FTC;
- the second comprising of an independent contractual right, with any monetary penalties then going to the suing company, as opposed to the FTC.

Ultimately, Snead observes that US companies and citizens are paying close attention to what's happening in Europe, with decisions such as that taken recently against Google helping to reinforce what is important about the GDPR – that is transparency, notice, and choice. While people may not like being told what to do, they understand the concept of penalties and the impacts on business.

Leveraging the Shared Concepts of Industrialized Democracies

As underlined by the comments of several participants at the roundtables, the issue of law enforcement access to data is essentially not just a US issue, but a global one. This is apparent, for example, in the EU e-Evidence proposal, or the German government's assignment of surveillance powers to the Bundesnachrichtendienst (Federal Intelligence Agency), including powers to act outside of Germany. While it is probably too ambitious to aim for global rules for law enforcement, David Snead and others suggested that leveraging the shared concepts of industrialized democracies (rule of law, general

protection for civil liberties) could lead to a joint approach, such as that incorporated in the CLOUD Act (also discussed here in interview with the eco Association and i2Coalition), which was passed in order to address concerns about how the US government was accessing data. In this regard, Peter Schaar speculated that future US administrations could be more open to negotiations with the EU on e-Evidence and CLOUD Act cooperation between both sides.

Moving Forward

In wrapping up the roundtables, Hirsch and Süme both referred to the good news that the appointment of the Ombudsperson appears to be concretely underway. Hirsch indicated that the discussion on the Privacy Shield will be on the agenda of the next European Parliament session.

While the roundtables had served to highlight room for improvement in the Shield, the conclusion concerning their overall message was that, in comparison to the situation pre-GDPR, a positive process of evolution is now evident, and that these improvements should be in the focus of any discussions in the EU Member States going forward. Ultimately, actions which jeopardize the agreement are regarded as running the risk of doing far more harm than good.

To bring the discussion to the next level, a third roundtable of the Transatlantic Dialogue is planned to take place in Washington in spring of this year.