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

Report on the 3rd Roundtable Dialogue in Washington D.C.

Representatives of the Internet industry from Europe and the US, along with US policy-makers, came together in Washington D.C. on 22 May to pave the way for better transatlantic data protection.

The Washington event was the third and final gathering in a roundtable series which began on February 7th in Brussels, then continued to Berlin on February 12th. All three roundtables were jointly hosted by eco – Association of the Internet Industry and the US based Internet Infrastructure Coalition (i2Coalition). The core focus of the roundtable 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.

Importance of SMEs to the Economy – and the Importance of Legal Certainty for SMEs
The Washington roundtable was opened by Christian Dawson, Executive Director of the i2Coalition, and Oliver Süme, Chair of the eco Association and Partner with Fieldfisher. Dawson started by highlighting that the i2Coalition and the eco Association are effectively the respective voices for the Internet on both sides of the Atlantic. This role includes conveying to regulators and legislators the economic importance of the Internet industry, and that this industry is made up predominantly of small to medium-sized enterprises (SMEs). As such, when legislators discuss how the Internet needs to evolve and how regulations might need to change, they need to take into account the needs of SMEs, who ultimately fuel the digital economy.

Oliver Süme echoed Dawson's sentiments, adding that he regards the digital economies on both sides of the Atlantic as mutually dependent. As Süme stated, this also stems from the fact that, in Europe, SMEs make up the backbone of the economy, accounting for 99 percent of companies, around 80 percent of employment, and 57 cent of every Euro of added value. While larger European corporations may already be clients to US cloud providers, the majority of SMEs are only at the cusp of going digital, with this signifying massive opportunities for US providers – but only if data can be transferred with legal certainty. As such, Süme essentially views legal certainty in the area of international data transfer as being one of the most important prerequisites for the further growth of digitalization in both continents.

The US Department of Commerce's Stance on the EU-US Privacy Shield
As a prelude to the panel discussion, Andrew Steele of the US Department of Commerce, specializing in International Trade Administration, briefed the meeting on the Department's perspective on the EU-US Privacy Shield. Steele recounted how, since being first instituted in 2016, the Shield has seen 4,600 US organizations become self-certified participants, and these numbers continue to grow. The success of the Shield, to which the administration remains firmly committed, has meant that a greater number of companies have made enforceable commitments on the protection of personal data from the EU, and that a higher number of both US and EU companies have access to tools that allow them to do business together. Ultimately, Steele regards the Shield as demonstrating that, for customers, it is imperative to have trust in the way that companies collect and process data. While a company's decision to self-certify is voluntary, once it has publicly committed to the process, its commitments are enforceable under US law through either the Federal Trade Commission (FTC) or the US Department of Transportation, depending upon which entity has jurisdiction.

The US government has assigned a team to work on cross-border data protection and has a team leader dedicated exclusively to the efforts to advance the Shield. In the area of awareness-raising, roadshows have already been held in 19 cities across the US, meetings have been held with over 200 companies, and 20 webinars have been broadcast. Due to the rigor of the certification process, not all companies achieve certification, with guidance on the process available at privacyshield.gov. The team conducts random spot checks and monitors news, with formal questionnaires being issued to participant organizations where credible evidence exists of non-compliance with the Shield. Misrepresentation on behalf of companies is prohibited, and referrals on false claims have already led to FTC settlements.

Steele also addressed the crucial question of the appointment of the Privacy Shield Ombudsperson, informing the gathering that, once confirmed by the Senate, Keith Krach, Under Secretary for Economic Growth, Energy and the Environment will assume this role, which will entail his processing of requests of EU and Swiss citizens relating to the transfer of data.

As Steele noted, a natural area of interest for the dialogue is the relationship between the Privacy Shield and the EU General Data Protection Regulation (GDPR). Whereas the Shield was introduced before the GDPR came into force on May 25th, 2018, it was designed with an eye to the GDPR and addresses both the substantive and procedural elements of the new law. The GDPR provides for continuity of prior EU Commission adequacy determinations, including the Privacy Shield. The Annual Reviews are an exercise in the Shield's framework which call for these adequacy reviews to be completed each year.

As Steele reported, the second Annual Review of the Privacy Shield, undertaken by both the European Commission and the European Data Protection Board in Brussels in October 2018, concluded that the Shield's framework offers an adequate level of protection for personal data transferred from the EU to the US. Substantively, the Privacy Shield is designed to bridge the gap between the US and the EU systems. While the privacy requirements are not identical, the Commission has found that the principles of the Shield are essentially equivalent to EU law requirements. While the Privacy Shield is not a GDPR certification mechanism, it nonetheless allows companies to comply with the data transfer provisions under Chapter 5 of the GDPR. Commenting further on the most recent Annual Review, Steele also welcomed the recognition of the efforts made to enhance the program and to address issues raised in the previous review.

Steele concluded by stating that information will continue to be shared with US organizations and the international community writ large, in order to help US organizations to maintain market access, promote their innovation, and support the transatlantic partnership, all within the scope of the GDPR.

Panel Discussion

The high-level panel discussion was moderated by Frank Stiff, Chair of the i2Coalition Board, and involved the following participants:

- **Melissa Froelich**, Committee on Energy & Commerce, Chief Counsel for Energy & Commerce Commission
- **Ned Michalek**, Chief of Staff for Congressman Eliot Engel, Chair of the Foreign Affairs Committee and Energy and Commerce
- **Ram Mohan**, CEO of Afilias
- **David Snead**, General Counsel for cPanel, and Policy Working Group Chair and Co-Founder of the i2Coalition
- **Andrew Steele**, US Department of Commerce and Specialist in International Trade Administration
- **Oliver Süme**, Chair of the eco Association, Partner & IT Lawyer Fieldfisher

Differences in Privacy Law: Background

Oliver Süme identified the different understandings of privacy and data protection in the US and Europe as having their underlying basis in cultural factors. Süme saw the definition of data protection in the GDPR as being a prime example of this variance, given that, under the GDPR, even an IP address can be considered to be personal data. Andrew Steele viewed the differences as stemming primarily from structural or regulatory approaches, with the process in the US being primarily sectoral. Here, he cited privacy laws which have been on the books since the 1970s, such as, in the healthcare space, the Health Insurance Portability and Accountability Act (HIPAA), as well as privacy regulations for education and for nonprofits. As Steele noted, as this body of law was already in place, it could be applied to the digital economy as it evolved. Given the robustness of existing privacy laws in the US, Steele does not necessarily endorse a focus on a single, comprehensive privacy law.

Implementation of Privacy Law: The Business Case

Ram Mohan referenced the significant burden facing businesses having to deal with different privacy regimes and expressed the hope that a common set of norms and rules would emerge. In weighing up such a burden, David Snead drew attention to the importance of metrics in understanding the benefits of privacy legislation for businesses. Referring to his own business experience, he reported that cPanel has more partners and distributors in the EU than in any other jurisdiction, and that the Privacy Shield is critical to cPanel in terms of demonstrating its commitment to taking its customers' information seriously. From a business perspective, he regards this as making Privacy Shield certification very valuable.

Outlook for Privacy Legislation in the US

Ned Michalek highlighted the current importance assigned to the topic of privacy legislation for many Members of Congress, fueled by concerns from constituents concerning data breaches and sale of information. As such, as Michalek speculated, while such legislation may not originally have been on the agenda for Frank Pallone (the Committee Chair of Energy and Commerce), it is likely that hearings will be held and legislation written given Europe's now stronger regulations. Michalek believes that what will ultimately drive the momentum for regulation is the growing realization that profitability stems from selling people's personal data.

Melissa Froelich also foresaw action on introducing legislation. In her opinion, the recently-introduced California Law has created more impetus in this direction than the long-standing debate around the GDPR and its implications. Froelich indicated that her bosses (Energy and Commerce Chairman Greg Walden and Cathy McMorris Rogers of the House Energy and Commerce Committee) were both advocating for one national standard, motivated by the need for transparency and accountability and, in particular, by the desire to head off risks for SMEs engendered by a potential patchwork of different state laws. Froelich continued by emphasizing the importance of data security in the ongoing conversation, with verification featuring as a key component of both the GDPR and the California Law. Apart from her own Committee, significant interest in privacy legislation is evident within the House, and 10 states are currently evaluating potential legislation. Froehlich regards this as representing a series of small but important steps forward.

How the Ecosystem can Influence Congress

Ned Michalek advised that the ecosystem should provide guidance to Congress concerning how they can craft legislation which is acceptable to constituents without crippling the industry. In his view, a collaborative approach is required, which contains an acceptance that refinements are always required.

According to Andrew Steele, stakeholder input is regarded by the US Department of Commerce as being crucial in shaping privacy legislation, with such input derived not just from large corporations and, interestingly, also not just from ICT companies. In point of fact, the majority of Privacy Shield certified companies are not categorized as ICT companies, with Steele echoing the earlier observation that the Internet economy is now synonymous with the economy itself. Steele reported on various initiatives being undertaken under the umbrella of the Department of Commerce to engage with stakeholders. In particular, the National Institute of Standards and Technology (nist.gov), has just held the second of three workshops on its own Privacy Framework. Its evidence-based approach, which can demonstrate what's palpably going to deliver benefits to the customer and society in general, represents the optimal route forward, according to Steele. The dialogue being led by NIST with computer science experts and risk engineers is feeding a terminologically precise process which addresses the question of what is trying to be achieved with data breach notification. According to Steele, this need to explain terms is of critical importance. While the GDPR has been extremely well thought-through, and represents a significant enhancement over the 1995 Directive, it still contains terms that are problematic (e.g. "state-of-the-art" or "disproportionate costs"), meaning that there will be ongoing conversations in which all stakeholders will need to engage.

David Snead underlined four principles which the i2Coalition hold as being imperative in the shaping of legislation: those of practicability, accountability, evaluation of legislative effectiveness, and system-wide application. Expanding on the topic of practicability, Snead cautioned that privacy notices should not be subject to a requirement for automation. On the subject of technology, Ram Mohan spoke about the potential of the successor to the WHOIS Protocol, the Registration Data Access Protocol (RDAP), which should allow companies to provide data based on configurable profiles. Mohan called for policy-makers to take account of such mechanisms and protocols to contribute to the harmonization of implementation across jurisdictions.

Learning from the California Law

Frank Stiff posed the question as to whether the California Law was likely to represent the standard for US legislation, noting that Nancy Pelosi has alluded to the toughness of this law. Ned Michalek observed that nothing unites business and Members of Congress more than a state moving ahead of Congress, before urging businesses to engage proactively in the process of achieving a national standard. His belief is that a patchwork system of legislation would be counterproductive.

While conceding that the California Law has some flaws, particularly in the area of verification (which she views as unsurprising, given that the bill was drafted and passed in seven days), Melissa Froelich views the law as constituting an interesting case study which could be learned from to shape a national standard. All in all, Froehlich expressed optimism that a bipartisan bill might be possible in the 116th Congress, an optimism which was shared by Michalek, who added that time was of the essence.

Learning from the GDPR

Oliver Süme pointed to the learning that the US could gain from the GDPR. From his perspective, while the GDPR represents a milestone and the most significant achievement in digital policy in the last 20 years, it nevertheless is also not without imperfections. A key lesson which should be heeded by other legislators is that the GDPR does not offer enough flexibility or sufficient exemptions. Even if one of its elements is to take a risk-based approach, it does not make sufficient distinctions between big and small companies. The complex legal requirements are leading to significant confusion, in particular for smaller companies.

Dealing with Multiple Privacy Regimes

Oliver Süme regarded the need to deal with multiple regimes as one of the biggest challenges confronting companies, particularly SMEs. The GDPR's provision for a number of "opening clauses" and, in particular, its allowing each nation state to determine how employee data in employment contexts is dealt with, exacerbates the complexity for companies working in multiple jurisdictions. For companies providing services within the EU, it is in some cases necessary to dig into the potential frameworks of each Member State, and this becomes even more complex for those also offering services outside of the European jurisdiction.

This complexity and fragmentation was regarded by Ram Mohan as representing the single biggest threat to privacy work worldwide. In his opinion, it is not privacy regulations that are likely to cripple business, but rather their disparate implementations. Referring once more to RDAP, he emphasized its benefits as an agnostic model in terms of its indifference to whether implementation occurs in a centralized or distributed manner or whether authentification is done by one or many parties. Mohan referred to a mechanism referred to as the TSG01 (technical model for access to non-public registration data), which is being undertaken by ICANN's Technical Study Group Document on Access to Non-Public Registration Data. This is endeavoring to set out a common model with the potential to allow businesses to implement a single specification. This would mean that, rather than data needing to be transformed, a framework could be applied with different filters.

While not dismissing the value of such mechanisms, David Snead suggested that the priority in policy-making should be on reaching a common understanding of what's collectively important in terms of privacy. This view found resonance with Andrew Steele, who pointed out that approximately 100 countries have data protection laws on their books. The GDPR has garnered most attention due to its reach (500 million individuals and potential customers) and the scope of its fines (4% of global annual revenue or up to 20 million Euro, with France already having imposed a 50 million Euro fine), with US companies alone having expended 7 billion dollars. If this is replicated around the world, it could be viewed as constituting digital protectionism, as it would make market access harder for smaller companies. If the goal is free exchange in innovation and competition, then interoperability is key. In Steele's opinion, this is what the Privacy Shield delivers as a tremendously valuable tool that serves as a bridge between two different regulatory regimes. Another such tool is the Cross-Border Privacy Rules system which applies to the Asia-Pacific Economic Community, which has now been adopted by 8 economies (the US, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, and Chinese Taipei) and which also takes cultural norms into account.

On the basis of such examples, Steele believes that it is possible to find a common approach which provides the foundations upon which can be built, with the best companies tending to use these voluntary mechanisms to differentiate themselves from companies who don't take privacy as seriously. Steele is of the opinion that we are now approaching a more robust global discussion about what the GDPR does or does not do right and about how the US can refine its approach by taking the sectoral lessons that have been learned and move forward.

Ram Mohan and David Snead both agreed that a framework of principles that would allow businesses to meet the needs of consumers would be welcome, with Mohan emphasizing that it is not the principles in themselves that are burdensome, but the implementation mechanisms, which he believes are contributing to a new privacy divide which is pushing smaller companies out of the game.

Oliver Süme also shared the view that there are many common approaches to the various international processes worldwide. He pinpointed three core principles that every privacy or data protection regime

is effectively dealing with: transparency; accountability and the obligation to document your processes; and strong data subject rights. In the European arena, Süme regards the mechanism that the European Commission applies to deal with other legal frameworks as being of particular interest: namely, the adequacy decision that the Commission can reach if they conclude that a country has a similar level of data protection, with this representing the easiest means for approval of data transfer. Süme concluded by expressing his optimism that, as many countries work on data protection, the European Commission will in future acknowledge more countries as having an adequate level of data protection, and this could potentially be the most elegant solution for legal data transfers.

In the meantime, for transfer of data between the EU and US, the priority should be to strengthen the Privacy Shield.