No consensus on Privacy Shield following debate on adequacy

March 2016

Authors: Detlev Gabel, Tim Hickman, Robert Blamires, Matthias Goetz, Audrey Oh

The EU-US Privacy Shield remains a hotly debated issue. At a meeting at the European Parliament last week, it became evident that significant areas of disagreement remain between the European Commission, the European Parliament, privacy activists and businesses.

Background

On 17 March 2016, representatives from the European Commission (the "**Commission**"), US Department of Commerce, Members of the European Parliament ("**MEPs**"), business groups, academics, and privacy activists debated key issues surrounding the proposed framework for transatlantic transfers of personal data from the EU to the US (the "**Privacy Shield**"). The debate highlighted the fact that there remain significant areas of disagreement as to whether the Privacy Shield is an improvement on the Safe Harbor, whether it meets the requirements set out by the Court of Justice of the European Union (the "**CJEU**"), and how to practically safeguard the personal data of EU data subjects being transferred to the US.

Main points of contention

Mechanism for Legal Redress

US Department of Commerce officials defended the proposed legal redress mechanism provided by the Privacy Shield. They outlined the numerous redress options that would be available to EU data subjects who consider that their personal data have been misused. For example, companies need to respond to complaints within 45 days and aggrieved data subjects will benefit from cost-free alternative dispute resolution. As a last resort, data subjects will have recourse to the Privacy Shield Panel, a dispute resolution mechanism that can take binding and enforceable decisions on US companies that receive personal data under the Privacy Shield. Furthermore, data subjects always have the option to complain to their local Data Protection Authority ("**DPA**"), which is empowered to refer complaints to the Department of Commerce and the Federal Trade Commission for investigation and enforcement in the US. By contrast, civil society representatives suggested that the legal redress mechanism under the Privacy Shield was potentially more complex than the system that existed under Safe Harbor, and that alternative dispute resolution is rarely viewed in a favourable light by consumer privacy associations in both the US and EU.

Independence of the Ombudsperson

MEPs scrutinised the role of the proposed Ombudsperson under the Privacy Shield. In particular, they questioned whether the Ombudsperson was truly independent, as compared to, for example, a judge. They questioned whether the positioning of the Ombudsperson in the executive branch of the US government would compromise his or her autonomy and leave him or her vulnerable to influence from the surveillance community and third parties. Civil society organisations also pointed out that under the proposed Privacy Shield system, the only mandatory responses to a complaint made by an EU data subject would be: (i) confirmation that an issue has been investigated; and (ii) assurances that either there has been compliance with the Privacy Shield or that the breach has been remedied.

Isabelle Falque-Pierrotin, Chair of the Article 29 Working Party (the "**WP29**" – an EU body made up of representatives from each national DPA) noted that the creation of the Ombudsperson role represents clear progress from the position under Safe Harbor, but commented that the Ombudsperson needs to be provided with real powers and must be truly independent. This may prove to be a key point in the WP29's forthcoming review of the Privacy Shield.

Legal Status of US Assurances

Questions were also raised regarding the reliability of the written assurances provided by the US government, whether the Commission had been right to rely so heavily on those assurances in its Draft Adequacy Decision, and what those assurances mean legally (especially with the approaching change in leadership following the US Presidential Elections). The Commission noted that these assurances are not made by US officials in their personal capacity – they are empowered to make commitments on behalf of the US government which are carried forward regardless of the administration in power. Department of Commerce officials assured sceptics that if the US ever walked away from its commitments, the EU could suspend the Privacy Shield and pull out of the agreement at any time without having to wait for an annual review.

Fundamental Rights vs Business Interests

Early last week, a group of consumer and civil society organisations (calling themselves the "**Privacy Shield Coalition**") published a letter outlining many of the same questions raised during the Parliamentary hearing. The letter declared that the Privacy Shield "manifestly fails" to provide for the conditions laid out by the CJEU and the WP29 for an agreement to meet EU standards for transfers of data to the US. Similarly, consumer advocate groups at the Parliamentary hearing argued that the proposed Privacy Shield framework was flawed and that it compromised the fundamental rights of EU consumers citing, for example, the absence of any provisions on data retention.

In contrast, supporters of the Privacy Shield advocating a business-friendly approach urged participants at Thursday's hearing to accept that the negotiated package was a pragmatic solution that should be implemented in a timely manner, in order to avoid any further disruption to trade and regulatory uncertainty that has persisted since the CJEU ruling in October 2015. For example, DigitalEurope came out in strong support of the Privacy Shield, and stated that it had full confidence that the Commission had adequately addressed the concerns raised by the CJEU and was committed to the Privacy Shield's success.

Conclusion and next steps

This debate highlighted the tensions between all stakeholders involved in the Privacy Shield. The pressing questions essentially boil down to whether the Privacy Shield agreement fulfils the requirements set out in the CJEU's ruling and provides sufficient protection for personal data that are transferred from the EU to the US, and if not, how to proceed in a pragmatic manner that minimises disruption to businesses and transatlantic trade.

Following written comments that are expected from the WP29 and the Parliament, the Commission is expected to finalize its Adequacy Decision on the Privacy Shield in June. Some privacy activists are already suggesting that if the Commission issues an Adequacy Decision in favour of the Privacy Shield, they will challenge that decision through the courts.

Against this backdrop, the General Data Protection Regulation (the "**GDPR**") is expected to be adopted later this year, bringing with it significantly greater penalties (up to €20 million, or 4% of annual global turnover, whichever is greater) for businesses that fail to abide by EU data protection law. In addition, the extraterritorial application of the GDPR means that companies based in the US but doing business in the EU may find themselves subject to the provisions of the GDPR, regardless of whether they have self-certified under the new Privacy Shield agreement. In this present state of uncertainty, businesses should continue to monitor developments closely.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000

In this publication, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law and all other affiliated partnerships, companies and entities.

This publication is prepared for the general information of our clients and other interested persons. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.