EUROPEAN LAW BLOG
NEWS AND COMMENTS ON EU LAW

ELB Blogpost 46/2023, 17 November 2023
Tags: EU-US Data Privacy Framework
Topics: Data protection and digital governance

In the Shadow of the European Court of Justice: The Luxembourg Conference on Transatlantic Data Transfers

By Kenneth Propp

The EU-U.S. Data Privacy Framework (DPF) has only just taken effect, but the agreement already is under attack at the Court of Justice of the European Union (CJEU). On 7 September 2023, French parliamentarian Philippe Latombe brought before the General Court a direct action for annulment of the European Commission adequacy decision relating to the DPF. The CJEU rejected Mr. Latombe's request for interim measures that would have precluded application of the DPF, but it has yet to address other issues in the case, including standing.

Austrian privacy activist Max Schrems, founder of None of Your Business and protagonist in the invalidation of the two predecessor EU-U.S. data transfer agreements, also has publicly promised to file a challenge to the DPF this fall. Schrems appears inclined to bring an indirect action in a Member State court – possibly in Austria – setting the stage for a preliminary reference to the CJEU. The stage is being set for the latest act in the long-running transatlantic privacy drama to play out in Luxembourg over the next years.

Against this backdrop, on 15 September 2023 the Max Planck Institute for Procedural Law (MPI), located in Luxembourg close to the CJEU, convened a timely conference to examine the EU-U.S. agreement in the context of European fundamental rights and data protection law. MPI's outgoing director, Professor Burkhard Hess, hosted the proceedings, which were co-organized by the author of this blogpost. This post reports on the proceedings.

The conference brought together senior EU and U.S. negotiators of the accord, judicial officials, data protection and national security law scholars, civil society representatives, and legal practitioners. One unusual feature was the inclusion of European and American

national security officials responsible for data privacy oversight within their agencies. This post summarizes the main points registered during the discussion.

Two principal topics dominated. The first was whether the introduction by the United States, through Executive Order (EO)14086, of a necessity and proportionality standard for U.S. national security collection of personal data transferred from the EU to the United States, would satisfy EU law. The second was how the reinforced U.S. oversight and redress mechanisms for addressing claimed violations of data privacy rights compared to the requirements established in EU law.

Speakers also touched on several related topics. Should the CJEU apply to data transfers to third countries its separate jurisprudence relating to retention of data by member state law enforcement agencies? Should it invoke as an interpretative aid the long-standing case-law of the European Court of Human Rights (ECTHR) on surveillance of individuals by security services? Should the CJEU take into consideration how EU member states conduct intelligence activities when it assesses counterpart US authorities? Finally, should it take into account that EU data is still travelling to authoritarian states such as Russia?

Keynote Addresses

Two speakers close to the DPF negotiations opened the proceedings. Both speakers highlighted features of the new agreement that adapted data protection requirements to the singular context of national security collection. They welcomed the European Data Protection Board Opinion on the draft adequacy finding

They recalled the goals of the negotiation – finding solutions to the conditions required by CJEU jurisprudence, notably the *Schrems II* judgment, and ensuring effective protections within the U.S. legal system. They pointed out that the creation of a new U.S. administrative tribunal, the Data Protection Review Court (DPRC), was the most effective way under U.S. law to meet strict EU requirements for redress for Europeans. They stressed that access to the DPRC is based on a low admissibility requirement; for example, an applicant need not show that he or she has been surveilled. They also drew attention to the DPRC's character as an independent body with binding powers, as stipulated in EO 14086.

The speakers also observed that intelligence services, which need to protect sources and methods for obtaining information, operate with inherent limitations on the extent to which persons can be notified of the fact that their communications had been collected. In this respect, in line with European Court of Human Rights rulings, the participation of a special advocate in DPRC proceedings representing the interests of the applicant is an

important safeguard compensating for such limitations and thereby strengthening the representation of European complainants, it was noted.

The keynote speakers drew attention as well to the provisions on necessity and proportionality contained in EO 14086. The EO regards incorporates the legal standard of necessity and proportionality, relying on factors similar to those developed by the CJEU when balancing the protection of privacy and public interests such as national security, they observed. The necessity and proportionality standard is widely recognized in international instruments including the 2013 OECD Privacy Guidelines, supplemented by the 2022 OECD Declaration on Government Access, the speakers noted. The latter, it was observed, recognizes changes required in the security context to limit rights to data access and rectification. . The U.S. speaker closed with a call for the CJEU to interpret its 'essential equivalence' standard for third country legal systems in a f way that took account not only of these OECD instruments but also of Council of Europe Convention 108+ and the surveillance jurisprudence of the ECtHR.

European Data Protection and Fundamental Rights Jurisprudence

Speakers on the first panel described the current transatlantic data protection environment as fragmented and pluralistic, and complicated by the uncertainty of approaching U.S. elections in 2024. One speaker observed that the CJEU has constitutionalized international data transfers, and applies to it a rigorous and strict standard of review, as evidenced in its 2016 Opinion on the EU-Canada Passenger Name Record agreement. In light of how CJEU case-law has evolved, the speaker noted, the CJEU could be more transparent about its methodology for addressing foreign law issues and clarify its standard for doing so.

Several speakers pointed to the OECD Declaration as a sign of increasing transatlantic convergence among liberal democracies on data protection requirements in the security context. At the same time, one speaker noted, the EU Court of Justice has not yet had to consider data transfers to authoritarian countries like Russia, an issue he predicted would eventually require its scrutiny.

A U.S. speaker described the U.S. Department of Justice's (DOJ) formal findings, contained in a 34-page memorandum, about the level of privacy safeguards afforded by European national security authorities when collecting foreigners' personal data – the mirror image of the European Commission's adequacy decision. A substantial number of EU member states authorize access to electronic communications sent or received from abroad, under lesser safeguards than are applied to surveillance of domestic communications, the memorandum found. For example, some of these foreign-focused intelligence

surveillance programs lack *ex ante* independent review, and some allow domestic bulk collection of such data – a practice now barred in the United States, a U.S. speaker pointed out. In addition, a U.S. speaker noted, redress mechanisms in many EU member states for complaints about intelligence surveillance are not empowered to issue binding decisions, or in some case even to entertain complaints by U.S. persons. The U.S. speaker highlighted that, in view of these divergences, the DOJ had applied a deferential standard in assessing European practices, expressly referring to the wide 'margin of appreciation' adopted by the ECtHR in its extensive surveillance jurisprudence.

European speakers described the interaction of ECtHR and EU data protection standards. They noted that prior to the 2009 Lisbon Treaty, which conferred binding primary law status on the EU Charter of Fundamental Rights (EU Charter), the CJEU had deferred to the ECtHR approach on state surveillance of data transfers. However, a European speaker pointed out, the European Convention on Human Rights, unlike the EU Charter contains no precise textual counterpart to the right to protection of personal data set forth in the EU Charter. Article 52 of the EU Charter requires that its provisions be given the same meaning as corresponding rights in the European Convention, while leaving room for more extensive protection. The result in recent years, they noted, has been a growing gap between the strict CJEU standard, as exemplified in its *Canada PNR* opinion and the *Schrems* jurisprudence. and the more deferential ECtHR standard,

The CJEU's law enforcement data retention case-law also may have an impact on the judicial challenge to the Data Privacy Framework, it was suggested. A European panelist described the evolution of the CJEU's jurisprudence through recent cases such as *Spacenet*, where the Court carved out several exceptions to the general prohibition on bulk data retention. Despite this evolution, the speaker noted pressure coming from several major member states for a new EU law that would take fuller account of law enforcement interests; the next Commission might pursue such a measure, he suggested. In parallel, the Commission and the United States are pursuing an international agreement on the transfer of electronic evidence for law enforcement purposes, adding a transatlantic dimension to internal EU dynamics on the subject.

The panel was asked whether it expected the CJEU to incorporate rulings since *Schrems II* into its eventual judgment on the Data Privacy Framework. A majority of the panelists anticipated that the CJEU could refer to the evolving legal standard for data retention in considering US national security surveillance. Moreover, it was suggested, the CJEU conceivably also could elaborate its views on the permissibility of U.S. national security bulk data collection in the EU, a U.S. intelligence activity that is subject to DPF safeguards.

Necessity and Proportionality in Foreign Surveillance Law

Following this overview of European jurisprudence, a second panel explored in depth how its necessity and proportionality standard might be applied to the DPF. As several speakers noted, direct surveillance – where intelligence agencies obtain personal data by their own means and not via request to commercial service providers – has not been addressed by the CJEU. The ECtHR, by contrast, has issued a series of judgments on the subject, e.g. the *Big Brother Watch* case.

It was suggested by one panel member that the Luxembourg court, in its *Schrems II* ruling (paragraph 180), conflated the concept of necessity and proportionality with legality, a separate principle requiring that there be a legal basis for government action. Another speaker noted that the articulation of the necessity and proportionality standard in Article 52 of the EU Charter does not include the word 'strict' but that the CJEU itself added that requirement in *Schrems II* (paragraph 176). Another panelist referred to the efforts of the European Data Protection Board, following the *Schrems II* judgment, to clarify the contours of necessity and proportionality in its European Essential Guarantees for Surveillance Measures recommendations.

The U.S. decision to impose the necessity and proportionality criterion on its foreign surveillance programs through a legal measure other than a statute (Executive Order) was consistent with the CJEU view of member state administrative decrees as having the quality of 'law', according to a European speaker. Executive orders have a long and important history in the United States, a U.S .speaker observed. That person also highlighted that Executive Orders are durable in the national security setting; several issued at the beginning of the Cold War still underpin the structure and operations of U.S. national security agencies. It was also pointed out that the independent U.S. Privacy and Civil Liberties Oversight Board would review the U.S. intelligence community's implementation of its commitments under the EO.

Several speakers commented that a new international norm for protection of surveilled persons outside national borders was in the process of emerging, and that the U.S. Executive Order could be an important contribution in this evolution. Neither CJEU nor ECtHR jurisprudence are sufficiently comprehensive standards to address the increasing 'internationalization' of government access to data, one panelist asserted. The panelist suggested that governments develop a new multilateral agreement granting a tribunal powers to apply necessity and proportionality, since both COE Convention 108+and the OECD Declaration on Government Access lack enforcement mechanisms.

Legal regimes governing law enforcement and national security data collection differ in significant ways, it was pointed out by a European speaker. Law enforcement must, in

judicial proceedings, disclose the information it has collected about an accused person. Intelligence collection, by contrast, is aimed at informing decision-makers about security risks – arguably a use of data that has less impact on individual privacy. Only if intelligence services transfer data to law enforcement does it become subject to the latter's disclosure rules. The speaker also highlighted that the necessity and proportionality analysis required by the GDPR in respect of data in the commercial context accessed by governments is not replicated in the EU's counterpart Law Enforcement Data Protection Directive. The latter rather instructs that data collection be "not excessive," a more liberal standard.

Oversight and Redress Mechanisms In Foreign Surveillance Law

The day's final panel discussed European and U.S. systems for oversight and redress of foreign surveillance activities. It was observed that the European Parliament's report and recommendations on member states' use of Pegasus surveillance spyware had spotlighted deficiencies in their intelligence oversight mechanisms. An underlying report by the EU's Fundamental Rights Agency (FRA) had found that only 15 member states currently had independent oversight. The speaker considered that adherence to COE Convention 108+ is a potential way of helping remedy this situation, since it applies in principle to national security activities and incorporates the necessity and proportionality standard. (The European Union, by contrast, has limited authority for national security.) The United States should consider joining this Convention, as it has other COE instruments including the Budapest Convention on Cybercrime, it was suggested.

The CJEU's burgeoning law enforcement and national security data protection jurisprudence had led the European Data Protection Board to expand its involvement in these areas, it was noted. A European speaker noted that the EDPB's opinion on the Data Privacy Framework exemplified this trend : the Board had provided a pragmatic assessment of the accord. The speaker pointed approvingly to the system of special advocates who would participate in the classified proceedings of the Data Protection Review Court. However, the speaker observed, analyzing the new U.S. commitment to necessity and proportionality had proven more difficult for the EDPB, since CJEU and ECtHR case-law diverge in a number of respects.

Another important actor is the U.S. Office of the Director of National Intelligence (ODNI), which plays a central role in implementing the new U.S. oversight system, according to a U.S. speaker. It has elaborated internal procedures that apply across the expansive U.S. intelligence community, and it has publicized how persons in Europe may lodge complaints about data access. The ODNI office, which is entitled to see all information

about a complaint, then examines and issues its findings, including instructions on how to remedy any failings identified. The speaker anticipated that most complaints would be appealed to the DPRC. ODNI plans to publish information on the disposition of complaints.

The U.S. government had to navigate a complex set of U.S. Supreme Court precedent in devising the form of the DPRC, according to a US speaker. The speaker explained that the tribunal was conceived as an administrative rather than a body because the 2021 *TransUnion* case likely would prevent a European who suspects he has been surveilled by the United States from meeting the standing requirement for recourse to an ordinary court. Reference also was made to another recent Supreme Court case (*Arthrex*) which had reinforced the principle that administrative judges must be ultimately politically accountable to the U.S. Executive Branch. This ruling, according to the speaker, underlay the U.S. decision to locate the DPRC location within the U.S. Department of Justice, while ensuring it would operate in a functionally independent way through protections contained in a DOJ regulation. Lastly, according to this panelist, vesting jurisdiction over surveillance complaints in the U.S. judiciary would have required enactment of a federal statute, and the U.S. Congress generally avoids legislation that could be viewed as affecting the President's foreign policy authorities.

Conclusions

The Luxembourg conference illustrated the complexity of the task ahead for the CJEU in adjudicating challenges to the EU-US Data Privacy Framework. On balance, the issues relating to oversight and redress appear to be more clear-cut than those relating to necessity and proportionality. Despite the U.S. procedures laid down in EO 14086 for translating necessity and proportionality into operational reality, a question remains whether these will measure up to the CJEU's strict – yet still evolving – standard. Continued criticism by privacy advocates of the changes made to U.S. surveillance activities continues unabated.

Other factors also could play a role the next time around at the Court. The CJEU is conscious of EU member states' dissatisfaction over its strict data retention jurisprudence and its expanding scrutiny of member states' intelligence programs. In addition, there is increased consciousness within the EU of weaknesses in some Member States' surveillance oversight mechanisms, as revealed by the Pegasus scandal. Finally, Brussels is beginning to focus on continued data flows to authoritarian 3rd countries, and not just to the United States. As the context surrounding the legal challenges to the Data Privacy Framework evolves, so too may the CJEU's jurisprudence.