Cryptographic Technologies in the Post-Schrems II Era

Sunny Seon Kang
Data Privacy Attorney

Roadmap

Provide context on:

- CJEU Case C-311/18, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (“Schrems II”)
- European Data Protection Board (EDPB)’s guidance on supplementary measures

Explain in plain terms:

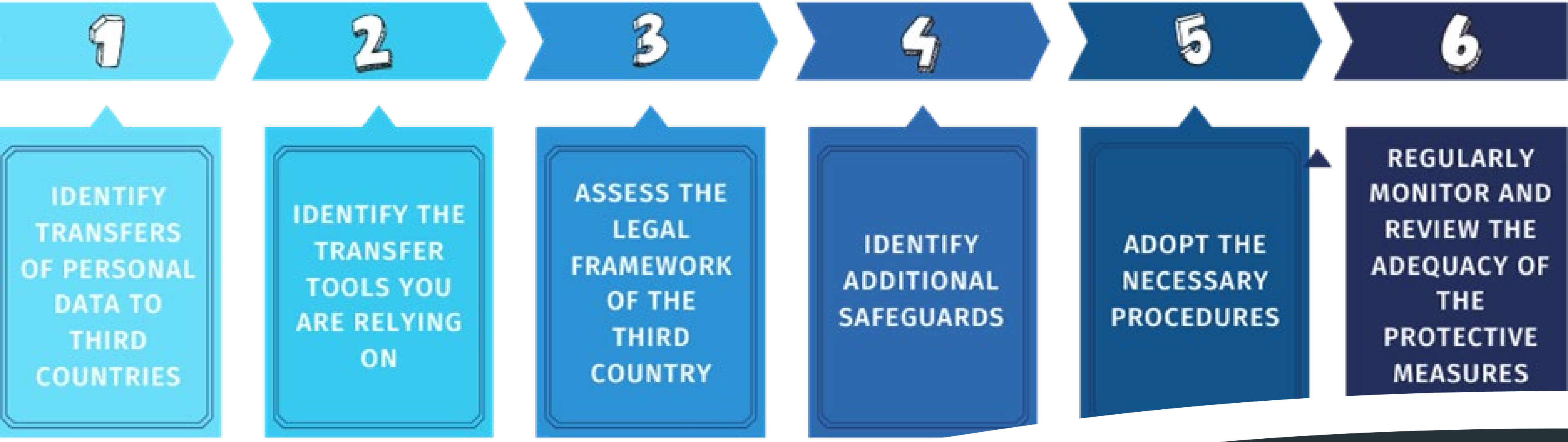
- EDPB recommendation on “split or multi-party processing” or “secure multi-party computation” technique

Policy discussion on:

- Supplementing legal safeguards with privacy-by-design
- Value propositions and obstacles in privacy-enhancing technologies

Standard Contractual Clauses: Necessary but not sufficient

- Schrems II: data importers must provide a level of data protection that is “essentially equivalent” to EU legal standards
- Standard Contractual Clauses (SCCs) are valid but not always sufficient
  - “By their inherent contractual nature cannot bind the public authorities of third countries”
  - To meet the “essential equivalence” standard SCCs may need to be supplemented with other technical, contractual, organizational measures.
- European Data Protection Board (EDPB) publishes guidance on supplementary measures in 11/2020



1

IDENTIFY TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES

2

IDENTIFY THE TRANSFER TOOLS YOU ARE RELYING ON

3

ASSESS THE LEGAL FRAMEWORK OF THE THIRD COUNTRY

4

IDENTIFY ADDITIONAL SAFEGUARDS

5

ADOPT THE NECESSARY PROCEDURES

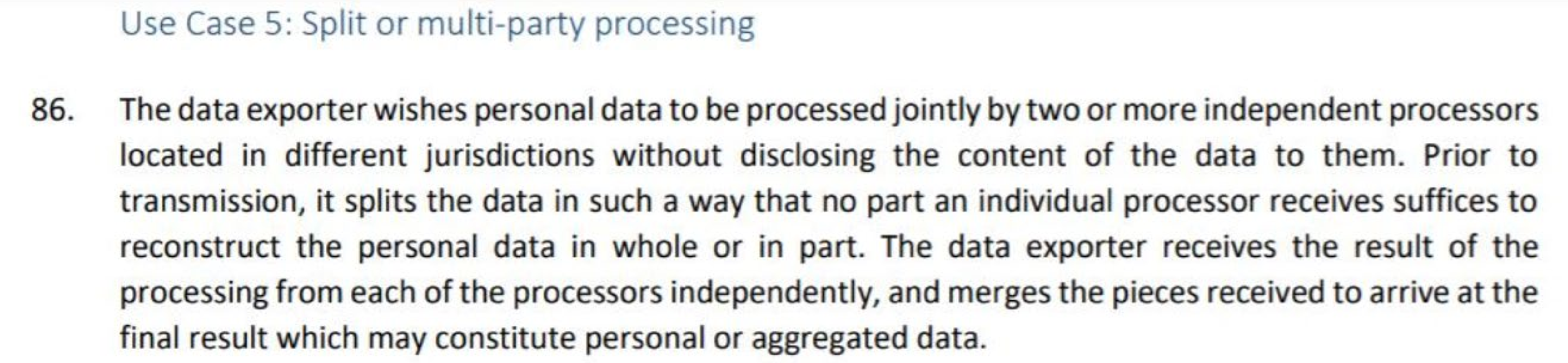
6

REGULARLY MONITOR AND REVIEW THE ADEQUACY OF THE PROTECTIVE MEASURES

EDPB Supplementary Measures Guidance 11/2020

So - what’s an example of a technical supplementary measure?

Secure Multi-Party Computation (MPC)



Use Case 5: Split or multi-party processing

86. The data exporter wishes personal data to be processed jointly by two or more independent processors located in different jurisdictions without disclosing the content of the data to them. Prior to transmission, it splits the data in such a way that no part an individual processor receives suffices to reconstruct the personal data in whole or in part. The data exporter receives the result of the processing from each of the processors independently, and merges the pieces received to arrive at the final result which may constitute personal or aggregated data.

Benefits of Decentralized Analytics in a Post-Schrems II Era

Security against Third Parties

Prevent the multiplication of data security and privacy risks inherent in third-party data transfers;

Privacy by Design

Self-execute fair information principles such as data minimization, purpose limitation, storage limitation, and privacy-by-design;

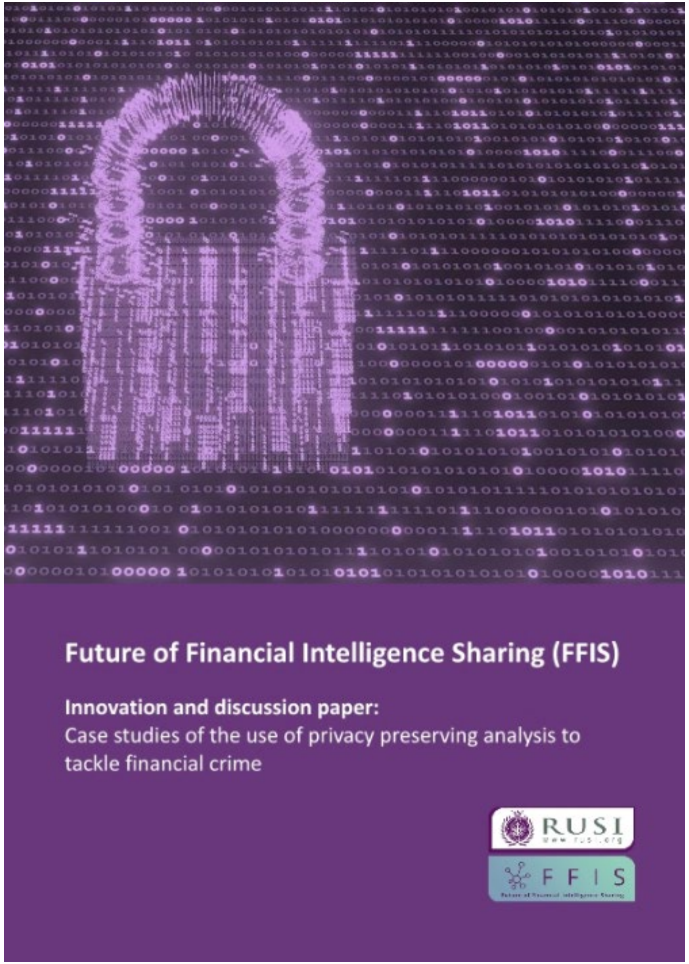
Information Sharing

Keep data resident in the premises of each data source whilst enabling collaborative computation—thereby advancing knowledge-sharing in cross-border environments.

Examples

- Financial information-sharing for anti-money laundering detection

- Diversifying input data for medical AI



Future of Financial Intelligence Sharing (FFIS)

Innovation and discussion paper:
Case studies of the use of privacy preserving analysis to tackle financial crime

So you might think: what’s the holdup?

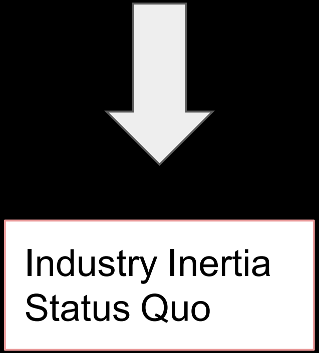
Challenges in privacy tech uptake

Fear of uncertainty

Regulatory guidelines are tech-neutral and thus shy away from specific compliance requirements of novel privacy-enhancing technologies

Overhead and Scalability

Cryptographic privacy tech may require significant configurations with the legacy system



Industry Inertia
Status Quo

Takeaways

Privacy-enhancing technologies still face challenges in implementation, but are becoming more relevant for EU-US data transfers:

- Assess the need for advanced privacy-enhancing technologies as part of the company's routine privacy impact assessment
- Depending on the nature of the data and the type of processing, contractual safeguards alone may not enough to prevent data leaks and breaches in practice. Cryptographic privacy-enhancing technologies can ensure a valid supplementary measure is in place for this transfer.