Asia-Pacific
Economic Cooperation

2021/CTI/SYM1/013
Session: 2

Personal Information: Protection and Data Flows

Submitted by: Bruegel

NEW ZEALAND
APEC 2021
ASIA-PACIFIC ECONOMIC COOPERATION 2021

Symposium on APEC Supporting the WTO Negotiations on Trade Related Aspects of E-Commerce
24-25 March 2021

Personal Information: Protection and Data Flows

J. Scott Marcus

Senior Fellow, Bruegel; Member, Scientific Committee, Florence School of Regulation / Comms & Media Programme (EUI); Fellow, GLOCOM (Japan)

The opinions expressed are solely my own.

Protection of Personal Information

- A brief reminder: What is at stake here?
- Different uses of personal data, different implications
- Cross-border flows of personal data: A difficult challenge
- Realistic goals
- Concluding thoughts

A BRIEF REMINDER: WHAT IS AT STAKE HERE?

The importance of personal data

- The WTO process on trade related aspects of e-commerce represents a unique opportunity to achieve some clarity at global level on a set of topics that are
  - increasingly important and yet
  - increasingly challenging.

- The use of personal data has always been important, but it has become an even more central theme due to:
  - The growth in power and influence of online platforms;
  - The importance of data as training corpora for artificial intelligence (AI) and machine learning (ML);
  - The growing criticality of e-commerce as a result of the COVID-19 pandemic.

Goals and trade-offs

- There is an inherent tension between
  - permitting as much exchange of data as possible in the interest of promoting economic gains, while
  - protecting the legitimate rights of the individual.
- APEC economies deal with this in one way or another, but they use different instruments and strike different balances.
- Any agreement will need to strike delicate balances between
  - being ***as ambitious as possible*** in drawing on those areas where a convergence of views is possible, while
  - enabling ***as many trading partners as possible*** to subscribe to the agreement and to fully implement it.

- How achievable is it for the most crucial trading partners to find common ground, and on what aspects?
  - The ***USA*** is home to many of the largest online digital platforms that are widely used worldwide.
  - The ***PRC*** is home to many large online digital platforms that are enjoying large and growing usage.
  - The ***EU*** is a major trading partner to both, and implements a robust protection of consumer privacy that applies to electronic services to its residents irrespective of where the services are hosted (and to which a number of other trading economies broadly subscribe).
- Any agreement that meets the needs of these three is likely to meet the needs of many other economies as well.

DIFFERENT USES OF PERSONAL DATA, DIFFERENT IMPLICATIONS

Personal versus non-personal data

- There are many different kinds of data:
  - Personal data
  - Non-personal private sector data
  - Non-personal public sector data
- For each of these, promoting as much use as possible has the potential to generate economic and social benefits.
- Our focus today is on personal data.

Different uses of personal data

- Personal data is broadly used by
  - Private firms for commercial purposes
  - Governments for public purposes
  - Governments for purposes of surveillance
    - For criminal justice
    - For national security

- These pose different risks for the protection of personal data.

Commercial use of personal data

- For the ***commercial use of personal data*** by private firms, there is more common ground than some might think.
- In the ***European Union***, protection of personal data is a human right that is anchored in the EU's founding treaties.
- In the ***USA***, there is no over-arching framework for the protection of personal data, but there are
  - Legal protections in sectors such as finance and health;
  - Detailed laws in many US states; and
  - A growing interest in creating a horizontal framework.
- In the ***PRC***, the there has been growing interest in recent years in strengthening the protection of the individual against increasingly powerful digital platforms.

CROSS-BORDER FLOWS OF PERSONAL DATA: A DIFFICULT CHALLENGE

Cross-border use of personal data: The EU as an example

- The EU arguably has the most developed jurisprudence on cross-border use of personal data, but for many economies, ***protection of personal data travels with the data***.
- The data protection rules put forward in the EU's General Data Protection Regulation (GDPR) apply to electronic services provided to Europeans, irrespective of where the services are hosted.
- The EU recognises countries that implement broadly equivalent protection of personal data by issuing ***adequacy decisions*** that permit unimpeded flow of personal data.
- Otherwise, flows of personal data to firms in third countries can be governed by ***Standard Contractual Clauses (SCCs)***.

Cross-border use of personal data: The EU as an example

- In July 2020, the highest court of the EU (the CJEU) ruled
  - that adequacy decisions must consider whether the use of personal data by foreign governments for surveillance is excessive, and whether EU persons have sufficient rights of appeal against improper surveillance;
  - that SCCs alone were not sufficient to permit the transfer of personal data to third countries, because they bind two firms but do not bind the foreign government.

Cross-border use of personal data: The EU as an example

- These CJEU decisions have posed some unique practical challenges to policymakers in the EU and the USA (and also in the UK).
- Different economies do not normally make commitments to one another about how they will implement surveillance on one another's citizens and residents.
- The USA had actually provided limited assurances to the EU in an set of agreements (Privacy Shield); however, the CJEU held them to be inadequate.
- Rights of appeal can hardly ever be exercised in practice because the individual does not know / cannot prove that he or she has been subject to government surveillance.

Cross-border use of personal data: The EU as an example

- The EU and the USA might quite possibly find a bilateral way forward, but a general international solution to these aspects of protection of international transfers of personal data is at best exceedingly difficult, and perhaps impossible.
- With all of this in mind, the EU might very well be able to agree on certain principles of data protection of individuals in a commercial context, but full agreement that permits transfer of data without additional measures seems unlikely.

REALISTIC GOALS

Realistic goals

- All of this seems to suggest that an agreement that includes the three most important economies might be possible as regards cross-border use of data for commercial purposes, but probably not for government surveillance.
- That the RCEP includes a brief section on cross-border use of data demonstrates that it is possible for very different economies to reach some basic (but limited) agreements.

Enforcement of protection of personal data

- Who would enforce the implementation of any agreements on the protection of personal data, and how?
- The WTO does not have demonstrated competence in this area, but it could conceivably enforce agreements if it is possible to agree to point to some standard that is recognised as having legitimacy.
- APEC has been a pioneer in this area – the APEC Information Privacy Principles are not a legally enforceable standard, but they might represent a good starting point.

CONCLUDING THOUGHTS

Concluding thoughts

- Otto von Bismarck described politics as “the art of the possible”.
- The negotiators of the WTO process on trade related aspects of e-commerce would do well to practice the art of the possible.
- Making headway in this very difficult area is likely to require
  - pragmatism,
  - flexibility,
  - creativity,
  - good will, and
  - lots of hard work.