www.worldcommercereview.com

Resolving the conflict between privacy and digital trade

Exports of data-based services by developing countries is threatened by the EU's privacy regulation. Aaditya Mattoo and Joshua Meltzer argue that the way forward is to reflect the EU-US Privacy Shield bargain

The EU's privacy regulation threatens developing country exports of data-based services by making data transfers more difficult. Traditional trade rules and regulatory cooperation cannot resolve this conflict. The column argues that the way forward would be to design trade rules that reflect the bargain struck in the EU-US Privacy Shield. Data destination countries would promise to protect the privacy of foreign citizens in return for source countries promising not to restrict data flows.

On 25 May 2018, the EU's new General Data Protection Regulation (GDPR) takes effect (European Union 2018). It has wider scope and stronger enforcement than the Data Protection Directive, which it replaces.

The current news focus on data leaks associated with Facebook, or on transatlantic data flows, have obscured the impact of GDPR on developing countries. Many developing countries export digitally delivered data-processing and business services, which require international flows of data. These services, ranging from financial accounts and tax returns to health transcriptions and diagnostics, contributed to more than $50 billion worth of developing country exports to the EU in 2015 – of which one-fifth came from Africa. Strengthened regulation makes data transfers more difficult, and so threatens some of these exports (Bauer *et al*. 2013).

Strengthened regulation

To ensure that the personal data of EU citizens is not abused, data can be transferred out of the EU only under certain conditions. One is that the country meets the GDPR 'national adequacy' requirement by enacting a national privacy law essentially equivalent to that of the EU. When GDPR comes into effect only Andorra, Argentina, Canada (for commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the US (using Privacy Shield) will have been recognised as adequate (European Commission 2018).

A national law imposes the same standard on all firms in the country, whether they handle EU data or not. This could adversely affect poorer countries. Prematurely stringent privacy laws could hurt the development of markets by inhibiting the flow of information. For example, the reporting of personal credit histories is critical to consumer credit, and privacy laws could create significant asymmetries of information and affect the efficiency of markets (Kitchenman 1999).

Traditional trade rules and regulatory cooperation cannot resolve this conflict... the way forward would be to design trade rules that reflect the bargain struck in the EU-US Privacy Shield. Data destination countries would promise to protect the privacy of foreign citizens in return for source countries promising not to restrict data flows

Enacting national privacy legislation would also increase the economy-wide cost of doing business. A recent survey suggested that, on average, members of the Fortune 500 would need to spend $16 million each on average to avoid falling foul of the new EU regulation (*Financial Times* 2017). The increased costs would hurt access to services at home and competitiveness in foreign markets where privacy is less of a concern. When the Philippines drafted national privacy legislation to ensure continued access to the EU data processing market, US firms based in that country suspended investment plans because operating costs would increase, leading the government of the Philippines to reassess its approach.

If a country's national law fails the EU adequacy test, as happened in the case of India, firms are required to use either Binding Corporate Rules (BCRs), designed for multinational companies to move data globally, or Standard Contractual Clauses (SCCs) for each business deal. Both instruments require levels of protection, oversight, and access for individuals that would be offered in the EU. Both also require a data controller or processor, who can be held liable for breach, to be established in an EU member state.

Both routes are costly and time-consuming. The requirement of a presence in the EU increases costs and limits the benefits of seamless cross-border digital trade, especially for smaller firms. A survey in India of the impact of the earlier, less-stringent EU Data Protection Directive revealed that the BCR process took more than six months, and 90% of the respondents used SCCs. These also involved a complex process and took on average more than three months (NASSCOM-DSCI 2013). Two-thirds of the surveyed services exporters claimed a significant loss of business opportunities because of the requirements.

Alternative routes to compliance

Is it possible to satisfy the EU's legitimate needs without obliging other countries to use EU standards in their privacy laws, or to incur the substantial compliance costs associated with SCCs and BCRs?

The tension between international data flows and divergent national privacy standards has provoked two types of international response: negotiation of trade rules, and cooperation between regulators.

- **Negotiation**. The WTO's General Agreement on Trade in Services (GATS) provides an exception for measures necessary to secure compliance with laws that are otherwise consistent with the GATS relating to *"the protection of the privacy of individuals in relation to the processing and dissemination of personal data"* (GATS, Article XIV(c)). The chapeau to Article XIV limits the exception to measures that do not lead to *"unnecessary and unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services"*. While the WTO panels and appellate body have made judgements in other cases on whether a measure was necessary to achieve a specific objective, it is probably unrealistic to expect an already strained WTO dispute settlement system to adjudicate the politically sensitive issue of privacy protection.

- **Regulatory cooperation**. Traditionally this implies harmonisation and mutual recognition. This is unlikely in this case and would not be sufficient to ensure international data flows. Harmonisation and mutual recognition of national regulations help firms create economies of scale, because they do not need to fragment operations to conform to differing regulations. But identical or mutually acceptable regulations do not, by themselves, address the central problem of international data flows. To protect the interests of their citizens, regulators in each country need to influence the behaviour of data-handling entities located outside their jurisdictions. The regulators in other jurisdictions who have control over these entities are not mandated to look out for the interests of citizens from other countries.

Instead of these traditional routes, it may be possible to build on a recent model of international cooperation.

- **Privacy shield**. When the EU first enacted privacy rules, it considered US laws inadequate, and transatlantic

data flows were threatened. In response, the EU and the US negotiated a Safe Harbor Agreement. This was updated after the Snowden revelations as the Privacy Shield Agreement (Privacy Shield Framework 2018). At the heart of this deal is a promise by US firms such as Microsoft and Google to protect the privacy of European citizens to European standards, in return for unrestricted data flows. This commitment is monitored and enforced by US institutions, notably the Federal Trade Commission and the Department of Commerce.

Since the EU has recognised US conformity assessment mechanisms under the Privacy Shield, WTO services law requires it to also grant other countries an opportunity to negotiate a similar arrangement. Developing countries can take advantage of the opportunity while strengthening their case for recognition by creating credible assessment institutions.

A recognition agreement with the EU would have big advantages over existing options. First, unlike in the case of BCRS and SSCs, firms would not be required to establish a costly presence in the EU because any assessment of conformity with EU standards would be done by domestic regulators. Second, unlike in the case of national adequacy, firms would not be obliged to adopt more stringent and more costly standards for data, involving transactions at home or with countries less demanding than the EU. Countries would be free to tailor domestic standards to domestic needs, and export standards to foreign needs.

First steps

We expect countries to proceed step-by-step in small groups, self-selecting into specific arrangements and gradually deepening them. As a first step, data source countries may still specify conditions and determine conformity unilaterally, but lend additional transparency and predictability to their requirements by listing them, for example as Additional Commitments under Article XVIII of the GATS.

A further step could be for data source countries to recognise conformity assessment in specific data destination countries when there is trust in enforcement,even though norms diverge. In parallel, groups of countries could also make collective additional commitments when they converge in regulatory requirements – say, in a WTO Reference Paper on Privacy – building on OECD and APEC principles (OECD 2013, APEC 2017).

These steps could pave the way ultimately for mutually binding obligations on source and destination countries, which is one of the most innovative elements of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). In this agreement, data source countries agreed not to restrict the flow of data, in return for legal obligations on data destination countries to protect the privacy of foreign citizens.

Apart from a bilateral or plurilateral approach, there may also be scope for multilateral discussions, for example as part of the recent initiative on electronic commerce. Such discussions could help forge a broader consensus on both data protection standards and mechanisms to ensure compliance. ■

Aaditya Mattoo is Research Manager, Trade and Integration, at the World Bank, and Joshua P Meltzer is a Senior Fellow at the Brookings Institution

References

Asia Pacific Economic Cooperation (2017), Privacy Framework.

Bauer, M, F Erixon, M Krol, H Lee-Makiyama, and B Verschelde (2013), "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce," European Center for International Political Economy.

European Commission (2018), "Adequacy of the protection of personal data in non-EU countries", accessed 22 May 2018.

European Union (2018), General Data Protection Regulation.
Financial Times (2017), "Global groups face big bills to comply with new privacy rules", 20 November.
Greenleaf, G, D Korff, and I Brown (2010), "Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments – Country Studies B.4 India," European Commission D-G Justice, Freedom and Security.
Glassman, CA (2000), "Customer Benefits from Current Information Sharing by Financial Services Companies," Financial Services Roundtable, December.
Kitchenman, WF (1999), "US Credit Reporting: Perceived Benefits Outweigh Privacy Concerns, The Tower Group."
NASSCOM-DSCI (2013), "Survey of the Impact of EU Privacy Regulation on India's Services Exporters."
OECD (2013), "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data."
Privacy Shield Framework (2018), Privacy Shield Overview.
WTO (1995), General Agreement on Trade in Services.

This article was originally published on VoxEU.org