2019

The GDPR's Effect on Transatlantic Relations

Christina Gay

The GDPR's Effect on Transatlantic Relations

Christina Gay

International Immersion Trip, Spring 2019

June 4, 2019

I. Introduction

Data protection is a rapidly changing field. Consequently, different nations' standards for using and managing data often vary drastically from one another. For example, the European Union (EU) and the United States (US) have taken substantially different views on what measures are necessary to protect data. The two nations have produced starkly divergent data protection laws, leading to inevitable conflicts whenever data is transferred from the EU to the US. The EU's new General Rules of Data Protection (GDPR) affects the majority of international trade that depends on data flows. It imposes new obligations on data processors before transnational transfer of European data can occur and has an extended territorial scope. Thus, third-party nations are put to the hard choice of whether to adopt their own nation-wide privacy regime in order to comply with the GDPR. The EU can use its market power to push other nations towards adopting its international data protection standard. This ongoing dispute over data protection has the potential to affect US domestic policy and the domestic policies of other third-party nations who wish to transfer data from the EU.

This paper argues that the convergence of third-party countries towards a GDPR-type privacy standard is both impossible and undesirable. First, many countries do not consider privacy a fundamental human right or, if they do, they must weigh privacy against other values, such as free speech, in ways that lead to lower levels of privacy protection than in the EU. Second, requiring third-party nations to either adopt a uniform privacy regulation or use firm-specific compliance in order to transfer data is too costly and burdensome for developing countries. This paper argues that third-party countries and the EU can build off of the EU-US Privacy Shield agreement as a means to resolve the conflict between regulatory heterogeneity and the desire for free international data flows. A recognition agreement with the EU similar to the Privacy Shield would be less costly for third-party countries and would not impose burdens on firms performing data transactions at home or

with nations other than the EU. Cross-border commitments could create a new framework for global privacy protection while supporting, not inhibiting, digital trade.

II. The EU's Approaches to Data Protection

The EU embraces a fundamental right of privacy for citizens, both online and offline. The notion that everyone has the right to protect her own personal data is plainly stated in the Charter of Fundamental Rights of the European Union, a document designed to explain the basic rights of European citizens and provide guidelines relating to those rights.[1] The European Convention of Human Rights also includes a right to privacy.[2] The fact that the EU attaches stringent protections to its citizens' individual privacy is not surprising, considering that most Europeans are only one or two generations removed from fascist or communist governments who strictly monitored their citizens' personal lives.[3] The EU experienced firsthand the dangers of governmental intrusion and then decided to provide sweeping safeguards for its citizens' individual privacy.

A. The Data Protection Directive

In October 1995, the EU agreed on a Data Protection Directive (DPD) to harmonize differing national legislation on data privacy protection.[4] The DPD is an omnibus legislation protecting personal data. The previous approach was fragmented country-by-country. The DPD sets out common rules for public and private entities in all EU member states that hold or transmit personal data. The DPD governs how information about European citizens can be collected and used across

[1] Charter of Fundamental Rights of the European Union Article 7, Oct. 26, 2012 (C 326) 393, 397 (explaining that "[e]veryone has the right to respect for his or her private and family life, home and communications." Article 8 concerns the protection of personal data, stating: "[e]veryone has the right to the protection of personal data concerning him or her.").
[2] Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, 312 U.N.T.S. 222, Art. 8.
[3] Theresa M. Payton & Theodore Claypoole, Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family, 250 (2014).
[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (Data Protection Directive).

industries, with each EU member state responsible for implementing the Directive through its own national laws.

The DPD provides that the transfer of personal data to a country outside of the EU may occur only if the European Commission determines that the country provides an adequate level of protection of personal data. The adequacy of a country's protections is assessed in light of all of the circumstances surrounding the data transfer, with particular focus on the nature of the data, the purpose and duration of the proposed processing operations, and the final destination's laws, rules, and security measures.[5]

B. The General Rules of Data Protection

The DPD succeeded in providing a cohesive framework for protecting citizen data privacy, but was considered inadequate by many in the EU because it was only a directive. In an effort to keep pace with technology, offer greater protection to EU citizens, and better harmonize data protection laws, the EU Parliament approved the final text of the General Rules of Data Protection (GDPR) in 2016.[6] It officially replaced the DPD on May 25, 2018. The GDPR is a uniform regulatory regime, ensuring that one system of data protection law governs the entire EU. Unlike the DPD, the GDPR is a regulation, which means that it is a binding legislative act enforceable as law in each EU Member State. Because it is a regulation, it did not need to be enacted into each country's legal framework. Upon implementation, it automatically resulted in one comprehensive data protection law in the EU, instead of twenty-eight. However, it does have several "opening clauses" permitting EU Member States to modify certain GDPR provisions.[7]

---

[5] Id.

[6] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[7] Id. The GDPR contains over 50 opening clauses, which allow EU Member States to put national data protection laws in place to supplement the GDPR. Basically, these clauses let Member States introduce more restrictive applications of

The GDPR has six key principles relating to the processing of personal data. It provides that personal data shall be:

> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').[8]

---

the GDPR via local legislations. Many EU Member States subsequently passed National Data Protection laws supplementing the GDPR.

[8] Id. at Art 5.

The GDPR also contains a broader territorial scope than the DPD. It applies whenever an organization physically operates anywhere in the EU, whenever data processed concerns an individual within the EU, or whenever the national law of a Member State applies to benefit public international law. It also enumerates stronger rights of control for data subjects and higher penalties for company violations.

The GDPR sets out to tackle the same goal as the DPD, protecting the fundamental rights of EU citizens concerning their personal data, but pursues the goal slightly differently. Data subjects covered by the GDPR receive remedial rights, including the right to compensation for controller or processor violations that result in damages.[9] For example, an entity who infringes a GDPR provision concerning cross-border data transfers is subject to administrative fines of 20,000,000 EUR or four percent of its worldwide annual turnover of the preceding financial year. For a multibillion dollar company, four percent of worldwide annual turnover can equal hundreds of millions of dollars. This is a very significant penalty for noncompliance with the GDPR. Thus, many companies are changing their data protection practices now to avoid enormous penalties later. The remedial rights embodied in the GDPR make the regulation's reach global.

C. Transferring Data to Third-Party Countries

Under the GDPR, data can only be transferred outside of the EU under certain conditions. The primary condition allowing for data transfer requires the European Commission to first find that the third country receiving the personal data provides an adequate level of protection.[10] Under Article 45, an adequacy decision enables data transfers to a third-party nation if the third-party can ensure that its country's data security standards are sufficient to comply with those in the EU. Adequacy determinations allow for the simplest process for data transfer because they require no additional

[9] Id. at Article 5.
[10] GDPR Article 45.

safeguards to be implemented by a business and no additional authorization requirements. However, an adequacy decision remains subject to periodic review by the European Commission.

The GDPR provides a comprehensive list of the considerations taken into account in making an adequacy finding. The considerations largely reflect those from the Article 29 Working Party approach.[11] The considerations include the existence of the rule of law, the existence of legislation on public security, whether there are effectively enforceable rights including administrative and judicial redress for data subjects, and whether there are international commitments entered into by the third-party country.[12] In practice, the third-party country must have a privacy regime in place that is essentially equivalent to the EU's.[13] This equivalence must relate not only to the level of data protection, but also to whether government agencies' access to personal data and data subjects' rights of redress are consistent with the GDPR's provisions.

More countries have begun to pass comprehensive data protection laws in order to receive adequacy determinations from the EU. However, the US has continued to follow a segmented approach consisting of specific agencies regulating certain types of data. Some US states have passed their own privacy laws, such as the California Consumer Privacy Act. But the US has not implemented a federal data privacy law that would open the door for an EU-US adequacy decision. However, the GDPR allows the European Commission to make an adequacy determination with respect to a single territory or particular sectors within a third country.[14] This opens the door for the Commission to find that specific states or economic sectors within a country provide an adequate level of protection for transfer. This enabled the EU and US to reach the EU-US Privacy Shield, serving as an adequacy determination only applying to specific economic sectors in the US.

---

[11] GDPR Article 41.1-2.
[12] GDPR Article 45.2.
[13] Schrems v. Data Protection Commissioner, Case No. C-362/14 (E.C.J. Oct. 6, 2015).
[14] GDPR Article 45.3.

If a nation does not receive an adequacy determination, there are still alternative options available to be able to transfer personal data outside of the EU. In the absence of an adequacy determination, the GDPR allows for data to be transferred outside of the EU pursuant to various safeguards or a derogation.[15] Companies that implement appropriate safeguards,[16] including Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), can legitimately engage in cross-border transfers. SCCs are standardized contractual clauses between two legal entities reviewed and approved by the European Commission. The biggest hurdle to implementing SCCs is the very high administrative costs associated with implementing hundreds of model clauses into each contract entered into by a company. BCRs are a compulsory code of conduct within a group of companies or enterprises engaged in the same economic activity. The final validation of a BCR can take over a year and also involves high expenses.

III. Negotiations With Third-Party Countries

The transatlantic economies are highly integrated. For example, commercial exchanges of goods and services between the EU and the US amount to nearly $1 trillion annually.[17] Both the EU and the US are deeply connected to the Internet; as a result, the largest intercontinental internet data flows are across the Atlantic. These data flows form the backbone of the transatlantic economy, both for direct e-commerce purchases of goods and services and for almost all business relations between the EU and the US. An enormous amount of data is exchanged between the US and the EU every

[15] The primary derogation is explicit consent. GDPR Article 44. Article 46 allows for cross border transfers of data absent an adequacy decision with the presence of appropriate safeguards. Article 49 lists appropriate situations for safeguards and derogations.
[16] GDPR Article 46: "a controller and processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on a condition that enforceable data subject rights and effective legal remedies for data subjects are available."
[17] CRS Report R43387, Transatlantic Trade and Investment Partnership (T-TIP) Negotiations, by Shayerah Ilias Akhtar, Vivian C. Jones, and Renée Johnson. See also CRS In Focus IF10120, Transatlantic Trade and Investment Partnership (T-TIP), by Shayerah Ilias Akhtar and Vivian C. Jones.

day, amounting to billions of dollars each year.[18] However, the GDPR's more stringent data protection requirements have the potential to disrupt these data flows. Due to the two nation's divergent data protection laws, conflicts will continue to arise when data is transferred to the US. This dispute has the potential to affect US domestic policy.

The GDPR's requirements will likely also affect domestic policy in third-party nations other than the US. Despite a claimed common interest in free data flows, the extraterritorial impact of Article 25 illustrates the EU's ability to exercise coercive market power on other nations. By using its considerable market power as bargaining leverage, the EU itself can strengthen other third-party nations' data protection laws. Third-party countries are essentially forced to either adopt similar data protection provisions to the GDPR or negotiate bilateral agreements. By using adequacy decisions as a barrier to enter the EU market, the EU privacy regime has succeeded in ratcheting up privacy protections in other countries.

A. EU-USA Privacy Shield

It took nearly five years for the EU and the US to agree upon the Safe Harbor in 2000 as a mechanism under which US firms could transfer personal data from the EU to the US in compliance with the DPD. Before reaching the agreement, EU's principal concern with allowing data transfers to the US was that the US lacked a generally-applicable law regulating the way in which firms can process personal data. As a general matter, the US Constitution, US statutory law, and US Supreme Court caselaw limit the extent to which governmental and law enforcement authorities can intrude into private space. Some laws restrict what private sector actors in specific sectors can do with personal data, in particular in the finance and healthcare sector. Similar laws have been enacted at the state level in various parts of the US, leading to a diverse picture of privacy law in the US. Thus, while in some

[18] Gregory Shaffer, Globalization and Social Protection: The Impact of the EU and International Rules in the Ratcheting Up of US. Privacy Standards, 25 Yale J Intl L 1, 39 (2000).

areas data protection rules are more stringent in the US than in the EU, there is no general requirement that data controllers or processors obtain unambiguous personal consent from individuals before using their data in each economic sectors.

Because the US does not have a general law protecting personal data, the European Commission did not approve the US as an "adequate" destination under the DPD. However, the two parties agreed on a mechanism that would allow certain US companies to meet the "adequate level of protection" required by the DPD. The Safe Harbor Privacy Principles, issued by the Department of Commerce in 2000, was a creative solution to allowing data flows to continue.[19] Under the Safe Harbor, US-based companies can receive personal data from the EU if they use one of the following mechanisms: join the EU-US Privacy Shield program, provide appropriate safeguards (i.e. contractual clauses or binding corporate rules), or refer to one of the GDPR's derogations. Around 4,500 firms pledged to adhere to the Safe Harbor principles and were consequently considered "adequate" for personal data transfers.[20]

The Safe Harbor was invalidated after revelations by Edward Snowden about the US government's ability to access data held by companies.[21] Five thousand companies previously relied on the now-invalidated measure to ensure successful data transfers.[22] Fortunately, just as economic necessity drove the US and the EU into the first Safe Harbor agreement, it drove them again to craft a new agreement. The US government and the EU eventually reached a new deal: the EU-US Privacy Shield.[23] The Privacy Shield arrangement places even more stringent obligations on firms that transfer personal data to the US. It includes stronger obligations for companies handling data, increases

[19] 65 FR 45665.
[20] Natalia Drozdiak and Sam Schechner, EU Court Says Data-Transfer Pact with US Violates Privacy, WSJ October 6, 2015.
[21] FTC, US-EU Safe Harbor Framework, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.
[22] Natalia Drozdiak and Sam Schechner, EU Court Says Data-Transfer Pact with US Violates Privacy, WSJ October 6, 2015.
[23] FTC, Privacy Shield, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield.

transparency regarding how data is used, safeguards against US governmental access to data, and provides new protections and remedies for individuals. It is based on self-certification by firms that they will comply with key privacy principles. In 2016, the Privacy Shield agreement was modified to clarify issues related to transfers to third countries and provide more explicit data retention terms. These changes led to an adequacy decision on July 12, 2016, just as the 14th Transatlantic Trade and Investment Partnership (TTIP) round began.[24] However, the Privacy Shield remains widely contested, especially in light of the changes brought on by the newly enacted GDPR. The Privacy Shield is being reviewed by the EU's European Court of Justice in light of the GDPR; if the US's privacy regime is again found wanting, a new and even more acrimonious debate is likely to occur.

The US will likely continue to hear chastening from European regulatory bodies, which may lead to changes in the US's data protection regime. States have begun to pass their own privacy legislation. In addition, in response to the Facebook-Cambridge Analytica debate, several members of Congress drafted federal regulations mirroring the GDPR and suggested the possibility for US standards based on EU principles. It is still unclear how the moving pieces in the global privacy regulation world will settle. If EU data privacy regulations take the day, they could influence more than just multinational corporations with EU customers. The tug of war between the US and EU on the validity of the Privacy Shield will continue to signal the strength of EU's convictions and the future of global privacy legislation.

B. Other Countries

The US is not the only nation entangled in the EU's prohibitions on the transfer of personal data — the European Commission has only found a few countries outside of Europe as providing adequate protections. Thus far, the European Commission has recognized Andorra, Argentina, Faroe

[24] EU-US Data Transfers, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay as providing adequate protection. The EU's decisions on Canada and the US are only "partial" adequacy decisions, meaning that data transfers to Canada and the US are still limited by various safeguard requirements. The adequacy decision on Canada only applies to private entities falling under the scope of the Canadian Personal Information Protection and Electronic Documents Act.[25] The EU-US Privacy Shield framework is a "partial" adequacy decision: only companies committing to abide by it benefit from free data transfers.

The EU desires to increase the number of adequate countries for transfer and is using its enormous weight as a trading power to encourage other countries to adopt strong data protection rules. For example, data protection was a major issue in the recent EU–Japan trade agreement finalized in the beginning of 2019. The EU sought to carve data protection completely out of the agreement, but Japan worried that its ability to sell digital products and services to the EU would be compromised without the certainty of an EU "adequacy" decision for data transfers to Japan. To secure an adequacy decision under the GDPR, Japan made data protection assurances to the EU and agreed to implement new rules to bring its data protection system in line with European regulations. Japan also created a framework for handling data-related complaints from Europeans. Consequently, in tandem with the finalized trade deal in January 2019, the EU issued a determination that Japan provides adequate protection for personal data. European Commissioner Vera Jourova stated that the new agreement between Japan and the EU created the "world's largest area of safe data flows."[26] This series of events could very well set a pattern for the EU's future trade negotiations.

---

[25] 2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002.

[26] EU-Japan Deal to Protect Data Exchanges Takes Effect, France24, (January 1, 2019), https://www.france24.com/en/20190123-eu-japan-deal-protect-data-exchanges-takes-effect.

The European Commission may decide to reevaluate existing adequacy decisions, primarily in light of the new obligations in the GDPR. It may even decide to limit or withdraw agreements that fall short of the comprehensive agreement between it and Japan. In Canada, whose own partial adequacy decision will be reviewed in 2022, officials still remain wary of overhauling their domestic rules to mimic the EU's. However, politicians continue to hold parliamentary hearings to discuss potentially revamping their laws in case their privacy deal with the EU becomes jeopardized. If Canada loses its adequacy determination, Canada could certainly decide to quickly rewrite its laws to conform with the EU's desires.

Canada and Japan are examples of the EU exerting its soft power to compel compliance with its data protection standard. These massive steps in data privacy and transfer will undoubtedly have global repercussions. Other countries are already beginning to follow suit. The EU and South Korea are exploring the idea of an adequacy decision, which would create an even bigger flow of data between the EU and other nations. Only time will tell if this will lead to global cooperation in the realm of data privacy or an even more isolated approach as countries aim to create their own different brand of data security. Now that Japan has secured an adequacy decision under the EU's GDPR, which opened up a channel of free-flowing data between the two nations, several other countries could follow suit.

IV. Can Other Nations Conform with EU's Privacy Standards?

Advanced economies like Japan can afford and are able to take the steps needed to conform with the EU's privacy standards. For example, Japan set up an independent agency to handle privacy complaints in order to conform with the GDPR during negotiations for the new Japan-EU trade deal. But, for emerging countries, the cost and administrative burden of applying the EU privacy standards may be daunting. It also may be viewed as a form of imperialism. In countries like South Africa, whose domestic legislation is primarily based on the EU's rules, the changes brought by the GDPR may be viewed with hostile eyes as an example of the EU extending its powers in a form of imperialism. Yet,

despite third-party nations' dislike of the GDPR's influence, any country not working towards the GPDR's standards is left out in the cold.

The GDPR confronts developing countries with a dilemma. If they seek an adequacy determination, then they must enact a national privacy law essentially equivalent to that of the EU. Argentina, Uruguay, and a few other countries have chosen to do so. However, a national law imposes the same data protection standard on all firms in the country, regardless of whether they sell exclusively at home or also abroad. This uniform and stringent standard could have adverse effects on developing businesses who operate solely in developing markets. The GDPR standard, which may be appropriate in an advanced country with well-developed markets and comprehensive access to services, is not necessarily also appropriate in poorer countries. Stringent privacy laws could hurt the efficiency and development of financial and other markets by inhibiting the flow of information within the market. Enacting this national privacy legislation would increase the cost of doing business in the economy, which would hurt competitiveness in foreign markets that do not have EU-like privacy regulations.

In addition, regulatory approaches to privacy are really mediated by cultural norms and will inevitably have to vary across countries. For example, Nordic countries have traditions of transparency and have thus maintained digital public databases of individual citizens' salaries and income tax records. This disclosure of financial information would contradict the US's traditions and strict laws protecting financial information. However, the US makes criminal records public, whereas such information is not available across the EU. Many academic studies have documented cultural differences in opinions about privacy and their implications for policy. These cultural differences suggest that exporting the GDPR's one-size-fits-all approach to other nations with digital platforms may not be optimal to realize what other countries want in terms of data protection.

Unfortunately, the alternatives to imposing an EU-like standard in order to get an adequacy decision and comply with the GDPR impose the same costs. Both BCRs and SCCs require that a data

controller or processor who can be held liable for breaches must be established in an EU Member State. The requirement of an EU presence increases the costs of compliance for small firms and limits the benefits that could be gained from a cross-border digital trade. Developing countries are faced with the hard choice of accepting nation-wide EU standards or incurring the substantial compliance costs associated with BCRs and SCCs in order to comply with the GDPR.

A. India as an Example

The GDPR poses a challenge for a country like India. A significant portion of India's services exports rely on cross-border data flows. Nearly forty percent of India's exports consist of software and information-technology services.[27] Virtually all of these cross-border exports rely on international data flows. In order for India to provide these services, it often must collect data from EU citizens. So, its exports are heavily affected by changes in and compliance with EU's privacy laws.

India is in the process of developing its own privacy regulation, but it does not have a regime that would be deemed adequate by the EU. As a developing country, India's approach to privacy must balance the risks of breaches of privacy with the economic potential of data use. A national law would require all firms to adhere to the same stringent privacy standard regardless of which foreign or domestic market they serve. The result could be an economy-wide increase in the costs of doing business.

In the absence of an adequacy finding, firms in India would need to rely on BCRs or SCCs to access EU personal data. But BCRs and SCCs are costly. A survey in India of the impact of the less-stringent DPD showed that the BCR process took six months and the SCC process took more than

[27] Aaditya Mattoo and Sacha Wunsch, Pre-empting protectionism in services—the GATS and outsourcing, Journal of International Economic Law 7, (4), December 2004, at 765–800.

3 months.[28] The GDPR requirement for a physical presence in the EU in order to utilize BCRs and SCCs further limits opportunities for many businesses to use the internet to sell services globally.

V. Solution

Instead of these traditional approaches, it may be more fruitful to build on a relatively recent model of international cooperation. When the EU first enacted the GDPR, US privacy protections were deemed inadequate and transatlantic data flows were threatened. In response, the EU and the US negotiated a Safe Harbor Agreement, updated after the Snowden revelation as the EU-US Privacy Shield Agreement. The core of the deal is a promise by US firms to protect the privacy of EU citizens at levels equal to EU standards in return for unrestricted data flows. The bound companies' commitments are monitored and enforced by US institutions, primarily the FTC and the Department of Commerce. The Privacy Shield Agreement helps restore legal certainty in the transfer of data across the Atlantic, but there will remain a level of uncertainty until the Court of Justice rules on the underlying adequacy of democratic controls in the USA.

By recognizing US conformity under the Privacy Shield, the EU created a valuable opening for other nations. Importantly, the World Trade Organization (WTO) law on services trade requires that the EU must offer other countries an opportunity to negotiate comparable arrangements.[29] So, developing countries could take advantage of this opportunity to negotiate a similar agreement and strengthen their case for recognition.

This kind of recognition agreement with the EU would have big advantages over existing options. First, unlike under BCRs and SSCs, firms would not be required to establish a costly presence in the EU. Second, the assessment of conformity with EU standards would take place at home by

[28] NASSCOM-DSCI (National Association of Software and Services Companies—Data Security Council of India). 2013. Survey of the Impact of EU Privacy Regulation on India's Services Exporters.

[29] The General Agreement on Trade in Services (GATS) says that when two governments have agreements recognizing each other's qualifications, other members must also be given a chance to negotiate comparable pacts. The recognition of other countries' qualifications must not be discriminatory and it must not amount to protectionism. See Article VII.

domestic regulators. Third, unlike in the case of getting an adequacy decision, firms would not be obligated to adopt more stringent or costly standards for the data involved in transactions that take place purely at home or with countries that are less demanding than the EU. Countries would be free to tailor domestic standards to their own domestic needs and use different standards with different foreign needs!

Countries could self-select into specific arrangements, be it a EU-US Privacy Shield-like agreement or another mutually binding obligation on source and destination countries. As a first step, the data source companies could specify conditions unilaterally and determine conformity unilaterally, but also lend additional transparency and predictability to their own requirements by listing them for other nations to see. They could then go further and recognize conformity assessment in specific data destination countries when they trust its enforcement, even though their norms diverge. These steps could pave the way for mutually binding obligations on source and destination countries.

VI. Conclusion

The ability to move data freely across borders forms the foundation of successful international trade. However, the GDPR's mandate that countries either adopt EU-like national privacy regulation or require their firms to incur the costs of using BCRs and SCCs puts developing countries in a bind. This paper argues that regulatory convergence towards GDPR-like standards is undesirable for economic and normative reasons for developing countries. However, the EU-US Privacy Shield agreement offers a way to resolve the conflict. The Privacy Shield represents an innovative bargain: the data destination country promises to protect the privacy of foreign citizens consistent with their own national standards and in return the source country commits to not restrict the flow of data. This kind of cross-border commitment could help create a framework for global privacy protection while also supporting digital trade with developing nations.