LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

CBPR Forum Is An Opportunity For Global Privacy Framework

By **Jeremy Beutler and Taylor Osher** (May 4, 2022, 3:45 PM EDT)

Jeremy Beutler

Taylor Osher

Every day 2.5 quintillion data bytes are generated and sent all over the world. In 2021, this flow of data across international borders contributed $2.8 trillion to the global gross domestic product, and this figure is estimated to grow 45 times every 10 years.[1] Due to the immense value created through the globalization of data, businesses have an ever-increasing incentive to be able to share and receive data throughout the world.

On the opposite end of the spectrum, this mass sharing of information worldwide has led to consumer concerns over the privacy and safety of their information. As a result, some countries have created data privacy laws to limit cross-border data transfer practices.

The European Union's General Data Protection Regulation, which prohibits the transfer of personal data outside the European Economic Area without meeting specific safeguards, is the prototypical example of a data privacy regime that imposes restrictive measures on cross-border data transfers.

These conflicting views on how best to protect individuals' personal information while also balancing the economic interest shared by governments and businesses alike have resulted in different attempts to create a globalized set of standards to transfer data.

The U.S. Department of Commerce's recent announcement regarding the Global Cross-Border Privacy Rules Forum is one of the latest efforts to create a set of standards to promote global data flows while helping companies demonstrate compliance with internationally recognized data privacy standards.

The creation of the Global CBPR Forum comes on the heels of the European Commission and the United States' joint announcement that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework, or TADPF, that will replace the EU-U.S. Privacy Shield Framework that was invalidated by the Court of Justice of the European Union in July 2020.

As work is done to build out these frameworks, there is an opportunity to align them to provide businesses and consumers with consistent, globally recognized privacy standards.

The Global CBPR Forum

Built upon the Asian Pacific Economic Cooperation Cross-Border Privacy Rules that were established in 2011, the Global CBPR Forum is intended to promote a consistent approach to privacy while ensuring the free flow of data to promote economic development and regional integration.[2] The Global CBPR Forum will establish an international certification system based on the APEC CBPR.

Like the EU-U.S. Privacy Shield Framework, the APEC CBPR provides a means for businesses to certify adherence to certain privacy principles and for that certification to become legally enforceable through a privacy enforcement authority. In the U.S., the privacy enforcement authority under APEC CBPR is the Federal Trade Commission. Nine economies have joined the APEC CBPR: the U.S., Mexico, Canada, Japan, South Korea, Singapore, Australia, Taiwan and the Philippines.

Unlike some other international privacy frameworks, the APEC CBPR does not restrict international data transfer based upon domestic legal requirements. Rather businesses and organizations are free to develop their own internal business rules and policies that are consistent with CBPR requirements to gain certification. This business-by-business approach allows for consistency and accountability while also individualizing the privacy models needed to incorporate both developed and developing nations regardless of their domestic privacy laws.

A business participating in the APEC CPBR is required to implement data privacy policies and practices consistent with the APEC Privacy Framework. The APEC Privacy Framework establishes certain privacy principles, such as providing notice before collecting personal information, limiting the business's use of personal information to the purposes for which it was collected, and providing individuals with the ability to access and correct their information.

After establishing policies and practices consistent with the APEC Privacy Framework, an APEC CBPR accountability agent assesses the business to evaluate and ensure that the business's policies and practices meet the requirements of the APEC CBPR. Once the business's adherence has been certified, the certification becomes legally enforceable.

In addition, businesses must provide privacy complaint and redress mechanisms to individuals concerning violations of the certification. And a business that fails to comply with its certification could have the certification suspended or withdrawn and face enforcement actions by the privacy enforcement authority in their country (in the U.S., by the FTC).

Although the APEC CBPR saw adoption from large companies like Apple Inc., IBM Corp. and General Electric Co., fewer than 50 companies have been certified under the system.[3] Such limited adoption pales in comparison to the thousands of companies that had certified under the now defunct EU-U.S. Privacy Shield.

The new Global CBPR Forum will build upon the APEC CBPR framework but will be independently administered and separate from the APEC system, presumably to spur broader international adoption. Canada, Japan, South Korea, Singapore, Taiwan and the Philippines joined the U.S. in announcing the new Global CBPR Forum.

GDPR and the Trans-Atlantic Data Privacy Framework

A new data privacy framework is being promoted by the European Commission and the U.S. On March

25, they agreed to the TADPF. This comes almost two years after the Schremms II decision invalidated the EU-U.S. Privacy Shield Framework, leaving thousands of U.S. companies struggling to find an alternate legal means to continue their international business efforts with EU data while complying with the GDPR.

The exact terms of the TADPF are currently being translated into legal documents, but the framework promises to address concerns raised by the Court of Justice of the European Union in Schrems II regarding U.S. signals intelligence activities. Under the new framework the U.S. specifically must:

- "Strengthen the privacy and civil liberties safeguards governing US signals intelligence activities";
- "Establish a new redress mechanism with independent and binding authority"; and
- "Enhance its existing rigorous and layered oversight of signals intelligence activities."[4]

The EU and U.S. claim this new framework will allow data to flow freely and safely between participating companies. Other key principals of the TDAPF include a new set of rules to limit access to data by U.S. intelligence authorities to what is "necessary and proportionate to protect national security."[5]

These safeguards will be overseen by U.S. intelligence agencies, however, a new two-tier redress system will also be created to resolve complaints from Europeans regarding U.S. intelligence authorities' access to data and will include a Data Protection Review Court. The TDAPF retains the requirement to self-certify established by the EU-U.S. Privacy Shield Framework.

The Global CBPR Forum: An Opportunity for Consistency

The Global CBPR Forum provides benefits to businesses in that it allows for businesses to demonstrate their commitment to a common set of privacy standards, without the need for an entire country to be deemed as having adequate privacy protections.

One concern, however, is that through the development of another privacy framework, businesses continue to face a fractured regulatory landscape. The fractured environment imposes costs on businesses as they seek to navigate sometimes overlapping, sometimes conflicting, privacy requirements. And individuals face uncertainty as to how their personal information may be handled based on where the individual resides and to which entities (and jurisdictions) their personal information might be transferred.

Although the framework on which the Global CBPR Forum is based (i.e., APEC CBPR) has some similarities to the GDPR, it has notable differences and the APEC CBPR falls below the privacy standards set by the GDPR. For example, the APEC CBPR does not provide affirmative rights to individuals. The Global CBPR Forum has the opportunity to update and align these standards with the GDPR.

With the development of the TDAPF occurring at the same time as the announcement of the Global CBPR Forum, countries participating in the development of the Global CBPR Forum have a chance to align the Global CBPR Forum with the GDPR to create a privacy framework that can truly function globally. A framework that does not take into account the requirements under the GDPR limits its

usefulness and could simply create an additional, potentially conflicting privacy framework for businesses.

Aligning the Global CBPR Forum with the GDPR will have several benefits. First, a standard that aligns with the GDPR will create an increasingly consistent data privacy and protection standard for the treatment of individuals' personal information. This provides individuals in countries without domestic privacy laws (or limited privacy laws) with privacy protection when their personal information is handled by a Global CBPR Forum-compliant business.

Second, a standard that is consistent with the GDPR reduces costs on businesses by requiring that they comply with a single standard, which avoids the cost and effort associated with analyzing and complying with overlapping but different privacy regulatory regimes.

Third, a consistent standard, in compliance with the GDPR, has the opportunity to build brand recognition that benefits businesses and individuals alike.

Consumers are beginning to educate themselves and make economic decisions based on a preference for stronger privacy protections. An example of this comes from a 2019 Consumer Privacy Survey conducted by Cisco Systems Inc., which surveyed 2,600 individuals from Europe, Asia and the Americas to assess consumer interest in their privacy. In this study 91% reported that they would not buy from a company if they do not trust how their data will be used.[6]

The study also found that just over 67% of respondents were willing to "spend time and money" to protect their data, that they "expect to pay more" for better privacy practices, and that it "is a buying factor for [them]." Another 48% of those respondents, or 32% of the entire study, reported that they had already "switched companies or providers over their data policies or data sharing practices."

A framework that builds recognition with the public for providing strong privacy protections is something consumers can rely upon and feel good about when doing business with a foreign organization, regardless of the protection they may or may not receive from their own domestic privacy laws. In this way a consistent framework can uphold one of the intentions of the CBPR, which is to create a framework that can be used by nations of any size or at any developmental stage.

The benefits of brand recognition do not end with the consumer, however. As emphasized by the Cisco study, consumers are beginning to make decisions on who to do business with based on the strength of their privacy practices and are willing to spend more to get more. A consistent framework with brand recognition can become an advertising tool for businesses, further incentivizing them to certify with the framework recognized by consumers, rather than whatever framework is cheapest or easiest for them to implement.

A consistent standard also allows for the freer flow of information across borders, which supports growth of the digital economy.

It remains to be seen how the Global CBPR Forum will align or diverge with the GDPR and the TADPF, but it has the opportunity for member economies to signal to the world that there are benefits to creating a consistent framework for cross-border data flows.

Jeremy C. Beutler and Taylor Osher are associates at Stubbs Alderton Markiles LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://globaldataalliance.org/wp-content/uploads/2021/07/gdafactsandfigures.pdf.

[2] http://cbprs.org/about-cbprs/; https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

[3] http://cbprs.org/compliance-directory/cbpr-system/.

[4] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

[5] https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100

[6] https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf; see also https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative (in a survey of 1,000 North American consumers, finding that "consumers are becoming increasingly intentional about what types of data they share—and with whom").