17 January 2020

WHAT DOES THE USMCA MEAN FOR A US FEDERAL PRIVACY LAW?

A White Paper by the Centre for Information Policy Leadership (CIPL)[1]

On January 16, the United States Senate voted to approve a new trade agreement between the United States, Mexico and Canada -- the "United States-Mexico-Canada Agreement" (USMCA),[2] sending it to the President's desk for ratification. This agreement contains provisions that are directly relevant to a potential federal U.S. privacy law. The USMCA formally recognizes the validity of the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system, a comprehensive certified privacy program and cross-border transfer mechanism for personal data developed by the 21 member economies of APEC. The United States was instrumental in developing the CBPR and currently participates in this system. In light of the USMCA, any new comprehensive federal privacy law must take account of and enable the CBPR and similar formal accountability mechanisms, such as privacy codes of conduct and certifications, in order to fully account for U.S. obligations under the digital trade chapter in which this recognition is found. Moreover, such formal privacy programs and certifications should be included regardless of the USMCA because they are important tools for effective legal compliance, serve as cross-border transfer mechanisms for data flows to and from countries that require such transfer mechanisms, and deliver many other benefits to all stakeholders, as discussed below.

1. The USMCA recognizes the CBPR as a valid privacy certification

Article 19.8 in the USMCA's chapter on Digital Trade (Chapter 19) requires all three countries to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade," and that in developing this legal framework they "should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)."[3] It also encourages each country to develop "mechanisms to promote compatibility" between their different legal regimes for protecting personal information. Importantly, it states that "[t]he Parties recognize that the APEC Cross-Border Privacy Rules (CBPR) system is a valid mechanism

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 89 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Mexico ratified the USMCA in June, 2019. As of publication, Canada has not yet ratified the USMCA, but is expected to do so in late January, 2020.

[3] United States-Mexico-Canada Agreement, Article 19.8, *available at* https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between

to facilitate cross-border information transfers while protecting personal information."[4] In addition to recognizing CBPRs, this language strongly supports recognizing the broader concept of accountability tools such as privacy codes of conduct and certifications in a U.S. privacy law.

2. What are the CBPR?

As noted, the APEC CBPRs are a privacy certification developed by the 21 member economies of the APEC forum. The specific program requirements of this certification implement the nine APEC Privacy Principles set forth in the APEC Privacy Framework. APEC focuses on promoting trade throughout the Asia-Pacific region through a wide range of committees, working groups and their various projects and initiatives.[5] The CBPR are one such initiative. They were finalized in 2011 and are now being implemented and operationalized across the APEC region.

The principal purpose for the CBPR was to create a cross-border transfer mechanism for personal data for the APEC region in anticipation of potential transfer restrictions some APEC member economies might impose through their privacy laws. In such cases, the CBPR would serve as a valid mechanism to transfer personal data nonetheless. Critically, if domestic obligations exceed those established under the CBPR, those obligations must be followed in combination with those established under a CBPR certification. In this way, CBPRs can be made to work with any privacy regime, thereby promoting interoperability across borders. In addition, the CBPR function as a comprehensive privacy program that can deliver compliance and accountability for purely domestic purposes as well. So far, eight of the 21 APEC countries (U.S., Mexico, Canada, Japan, the Republic of Korea, Singapore, Chinese Taipei, and Australia) are participating in the system.[6] The Philippines are expected to be approved for participation in the first quarter of 2020.[7] Further APEC economies are working towards joining the system as well.

Each participating economy must have at least one formally approved third-party certification body known as "accountability agents". These accountability agents review companies' privacy programs for compliance with the CBPR and certify such compliance, subject to annual review and recertification. The CBPR program contains specific requirements around Notice, Collection Limitation, Use of Personal Information, Choice, Integrity of Personal Information, Security

[4] *Id.*
[5] *See* About APEC, https://www.apec.org/About-Us/About-APEC (last visited Jan. 16, 2019); and What is the Cross-Border Privacy Rules System (April 15, 2019,) https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.
[6] *Id.*
[7] PH Joins APEC Privacy System (September 20, 2019), https://www.privacy.gov.ph/2019/09/ph-joins-apec-privacy-system/.

Safeguards, Access and Correction, and Accountability.[8] The US currently has two approved CBPR accountability agents.[9]

While certifying to the CBPR is voluntary, the CBPR become binding and enforceable on companies once they are certified. As a result, each participating APEC economy must also have a privacy enforcement authority that provides backstop enforcement, including across borders with participating counterpart enforcement authorities. The Federal Trade Commission (FTC) is the official CBPR backstop enforcement authority for the US and participates in the APEC Cross-border Privacy Enforcement Arrangement (CPEA) for that purpose.[10]

3. A Comprehensive U.S. Privacy Law Should Include Codes of Conduct and Certifications

As lawmakers in the U.S. continue to pursue a comprehensive privacy law, their proposed privacy bills should include provisions that enable formally recognized and enforceable privacy codes of conduct and certifications. Providing for such formal accountability mechanisms would serve several purposes:

(a) Give effect to USMCA's recognition in Article 19.8.6 of the CBPR as a valid privacy certification. If a federal privacy law were not to enable codes of conduct and certifications such as the CBPR, it would be at odds with the endorsement of CBPR in Article 19.8 of the USMCA.

(b) Give effect to the USMCA's commitment in Article 19.8.2 to take into account the APEC Privacy Framework when developing a legal framework for protecting privacy. The CBPRs were a mandate of the APEC Privacy Framework and are designed to implement it. A federal privacy law that does not enable CBPRs would be inconsistent with this commitment.

(c) Enhance the interoperability between the US privacy law and foreign counterpart laws, such as the EU General Data Protection Regulation (GDPR) and the Brazil Personal Data Protection Act (LGPD), which also provide for privacy codes of conduct and certifications, both for domestic compliance purposes and for cross-border transfer purposes. Similar mechanisms in a US privacy law could be made interoperable through appropriate

[8] *See* APEC Cross-Border Privacy Rules System Program Requirements, https://cbprs.blob.core.windows.net/files/Cross%20Border%20Privacy%20Rules%20Program%20Requirements.pdf.

[9] *See* TRUSTe Named First Accountability Agent for APEC Cross Border Privacy (June 25, 2013), https://www.trustarc.com/press/news_truste_named_first_agent_for_apec_cross_border_privacy/; and APEC Endorses Additional U.S. CBPR and PRP Accountability Agent (June 13, 2019), Hunton Andrews Kurth Privacy & Information Security Law Blog, https://www.huntonprivacyblog.com/2019/06/13/apec-endorses-additional-u-s-cbpr-and-prp-accountability-agent/.

[10] *See* APEC Cross-border Privacy Enforcement Arrangement (CPEA) (May 13, 2015), https://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Cross-border-Privacy-Enforcement-Arrangement.

instruments and tools, or even be recognized as compliant with such other jurisdictions, thereby facilitating the accountable free-flow of personal data across borders.

(d) Facilitate legal compliance and accountability for companies that participate in such enforceable codes of conduct or certifications. This feature would not only benefit the participating businesses, but also consumers and relevant enforcement authorities. Consumers will be helped because such programs provide additional layers of oversight and a more consistent and comprehensive approach to compliance. Consumers may therefore expect better privacy protections, transparency and accountability. Enforcement authorities can expect greater efficiencies in deploying their enforcement resources, as basic, front-line complaint handling responsibilities will be with third-party certifiers. Only the more complex disputes will go to the enforcement authorities. Also, the formal structure of such programs will help streamline investigations of alleged violations and drive down enforcement costs.

(e) Improve compliance for SMEs. SMEs typically don't have significant internal compliance staff and resources and thus could benefit from such formal external programs, which help translate complex legal requirements into practical and operational compliance steps. Also, the third-party certifiers and similar oversight bodies play a substantial role in getting participating companies into compliance. Codes and certifications can also be designed to be scalable to the nature and size of the business, ranging from the smallest to the larges organizations.

(f) Serve as a due diligence and risk-management tool for companies in connection with identifying and vetting service providers, vendors and other third-party processors. A privacy certification identifies companies as accountable organizations that have been vetted by an approved third party. This helps both the certified company in attracting business and customers as well the company that is looking for a service provider and must exercise due diligence in identifying qualified providers.

(g) Serve as a mitigation factor in enforcement contexts, whereby good faith efforts to comply with such schemes would be taken account in enforcement and fine-setting decisions by a privacy enforcement authority as, for example, is provided for by the GDPR. This would be a significant incentive (among other possible incentives) for organizations to make use of such mechanisms.

(h) Assist with implementing a broader accountability requirement that should also be included in a federal privacy law. Accountability is globally recognized as a key building block for effective privacy and data protection regulation and included in the GDPR and other existing and developing privacy frameworks. It requires organizations to (i) implement a comprehensive privacy program governing all aspects of collecting and using personal information and (ii) to be able to verify and demonstrate the existence and effectiveness of such programs on request. Having a comprehensive privacy program in

place is the foundation for compliance with all applicable privacy obligations established by law, regulation or other standard, is instrumental in placing the burden of privacy protection where it belongs – on the businesses – and is essential for creating trust in the digital economy and society. As such, any new US privacy law should require comprehensive privacy compliance programs. Formal codes of conduct and certifications would then be one of the ways in which companies could satisfy this requirement.[11]

4. Examples from Current Proposed Privacy Legislation and Existing US Privacy Law

A promising example of including such mechanisms exists in Senator Wicker's recently proposed United States Consumer Data Privacy Act of 2019 (CDPA)[12]. It would give the FTC the authority to approve third-party certification programs to create standards or codes of conduct for compliance with "1 or more provisions of this Act" including, therefore, for entire privacy compliance programs. Any organization that is certified by an approved certification program would be deemed in compliance with the relevant provisions of the Act that are addressed by that program. This could include CBPRs in so far as their substantive requirements are the same as the requirement of the CDPA or any other US law that incorporates this kind of provision.

Indeed, third-party certifications are not new to existing U.S. privacy law. They have been used for more than 20 years in the context of children's privacy. The Children's Online Privacy Protection Act (COPPA) includes a safe harbor provision that allows FTC-approved third parties to validate that organizations' privacy practices are COPPA-compliant.[13] If an organization complies with an approved third party's safe harbor program, they will be deemed to be in compliance with COPPA. There is no reason not to include a similar framework more broadly in a general federal privacy law. Also, the FTC, through its privacy consent orders, often imposes comprehensive privacy management and compliance programs on organizations. These compliance programs typically cover all aspects of data collection and use as well as all elements of organizational accountability. Including a general requirement to have accountability-based privacy programs in a US law would create consistency between the law and what the FTC currently expects companies to have by way of internal compliance processes.[14]

Finally, it is also noteworthy that organizational accountability exists in many other areas of US law, including anti-corruption, corporate fraud and white-collar crime, anti-money laundering

---

[11] *See* CIPL Accountability Q&A, July 3, 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf

[12] United States Consumer Data Privacy Act of 2019, Sec. 403, https://www.huntonprivacyblog.com/2019/12/03/senator-wicker-circulates-draft-privacy-bill/nc7/

[13] 16 C.F.R. 312.11.

[14] *See* CIPL white paper on Organizational Accountability in Light of FTC Consent Orders, November 13, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organizational_accountability_in_light_of_ftc_consent_orders__13_november_2019_.pdf.

and healthcare.[15] A U.S. privacy law should similarly leverage this concept both through a general requirement for companies to implement comprehensive privacy programs and through formal accountability schemes, such as codes of conduct and certifications.

Conclusion

The USMCA has now formally recognized the validity of CBPRs as a transfer instrument as well as called on the parties to develop interoperability or "compatibility" mechanisms between their different privacy regimes. It is therefore critical that drafters of US federal privacy legislation likewise recognize and enable use of the CBPR as a transfer mechanism in any new US privacy law as well as enable certifications and codes of conduct generally. In addition, as discussed, there are myriad of other important reasons why accountability, codes of conduct and certifications should become a core component of such new privacy law regardless of the USMCA.

If you would like further information or to discuss any of these issues, please contact Markus Heyder, Vice President and Senior Policy Counselor of the Centre for Information Policy Leadership (CIPL) at mheyder@huntonak.com and Matt Starr, Privacy & Public Policy Manager at CIPL at mstarr@huntonak.com.

For further information about CIPL, please visit www.informationpolicycentre.com and follow us on LinkedIn, Twitter and Facebook.

[15] *See* CIPL white paper on Organizational Accountability – Existence in US Regulatory Compliance and its Relevance for a US Federal Privacy Law, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_-_existence_in_us_regulatory_compliance_and_its_relevance_for_a_federal_data_privacy_law__3_july_2019_.pdf .