Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

September 24, 2020

Why We Need Interstate Privacy Rules for the U.S.

A CONCEPT PROPOSAL

Executive Summary

In the absence of a comprehensive federal privacy law that pre-empts disparate and inconsistent state privacy laws, a multistate interoperability code of conduct or certification may be the only way for organizations, particularly SMEs, to comply with an ever-increasing number of state privacy requirements. But the benefits of such a code go beyond compliance. It will also improve consumer trust, increase organizational accountability, and bolster states' limited resources to enforce their privacy requirements. The code could also require participating companies to comply with its requirements in all U.S. states, even where there are no state privacy laws in place, thereby harmonizing and raising the level of privacy protection across the U.S. Indeed, the vast majority of states do not yet have data privacy laws, but it is important to develop such a code before they do. The earlier it is developed, the better the code can deliver seamless and consistent privacy protections across the U.S., and possibly help shape a future federal privacy law as well.

I. THE ISSUE – AN INCONSISTENT PATCHWORK OF STATE PRIVACY LAWS AND NO FEDERAL LAW

It is unlikely that Congress is going to pass a comprehensive federal privacy law any time soon, much less in 2020. This is despite the significant progress that has been made over the last two years, including the introduction of a number of new privacy bills in both the House and Senate.[1] For the foreseeable future, organizations will likely be forced to live with a patchwork of sector-specific federal privacy laws[2] and an increasing number of state privacy laws with disparate and inconsistent requirements.[3]

An environment in which privacy obligations vary dependent on the state residency of the individual whose data has been collected would create significant compliance challenges, costs and lack of legal certainty for organizations, particularly small businesses, that may not have large legal compliance budgets. It would also inhibit organizations' ability to innovate and use data, as well as harm the highly competitive U.S. digital economy, particularly rapidly-evolving AI and machine learning technologies, which require economies of scale and the ability to access and use large data assets. If one state's law were to prohibit an innovative new use of data, an organization might choose not to pursue that innovation, even if other states permitted it.

---

[1] *See* e.g. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019); Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020); Information Transparency & Personal Data Control Act, H.R. 2013, 116th Cong. (2019); Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019).

[2] Some examples include the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which applies to healthcare providers and healthcare insurance providers, the Gramm-Leach-Bliley Act (GLBA), which applies to the finance industry, and the Children's Online Privacy Protection Act (COPPA), which applies to the collection of children's personal information.

[3] California passed the California Consumer Privacy Act (CCPA) in 2018, and Nevada (Senate Bill 220) and Maine (Act to Protect the Privacy of Online Customer Information) passed less comprehensive privacy laws in 2019. In 2020, privacy bills were introduced in 30 states and Puerto Rico, though no new laws were passed, due at least in part to states adjourning their legislative sessions early because of the COVID-19 pandemic. For more information see https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx.

As more states inevitably pass diverging privacy laws in the coming years, organizations will find it harder to develop single products, services and technologies for the entire country, and will be in dire need of a solution that streamlines and harmonizes compliance with this patchwork of state laws. While there are ongoing efforts to draft a model state privacy law,[4] it likely cannot provide sufficient consistency between state privacy laws on its own. Existing state laws and the inevitability that some states will opt for their own approach instead of the model law necessitate the creation of an additional mechanism specifically designed to provide consistency and interoperability between the states.

II. THE SOLUTION – AN INTERSTATE PRIVACY INTEROPERABILITY CODE OR CERTIFICATION

A potential solution to the challenge of a growing patchwork of state privacy laws could be a set of interstate privacy rules in the form of an **interstate privacy interoperability code of conduct or certification**.[5] Privacy codes of conduct and certifications generally allow organizations to demonstrate compliance with a law or set of laws by adhering to a specific set of privacy standards and build trust in B2B and B2C markets (see Section III below). A U.S. interoperability code or certification would provide organizations with a framework to streamline and simplify compliance with a patchwork of state laws in the absence of a federal privacy law. It would not only help resolve compliance challenges and provide legal certainty for organizations of all sizes, it would also facilitate uniform privacy protection for all American consumers, regardless of where they live. Specifically, an interstate privacy code of conduct/certification would have the following features and objectives:

- Establish a set of common data privacy and security standards that organizations could implement for their business in the U.S;

- Deliver enhanced transparency, legal certainty and consistent privacy protections to all Americans;

- Be modelled upon similar schemes that have already been developed by the U.S. and operationalized by U.S. companies, such as the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules ("CBPR");[6]

- Draw its substantive requirements from existing privacy laws, certifications and other frameworks such as state privacy laws, CBPR, the GDPR, proposed federal and state privacy bills and ISO standards;

- Be recognized in states' privacy laws, as well as in a future federal privacy law;

---

[4] National Conference of Commissioners on Uniform State Laws, Collection and Use of Personally Identifiable Data Act, August 19, 2020, available at https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=8c095b40-4a84-f639-97f8-e7aeba71bbad&forceDialog=0.

[5] The terms "code of conduct" and "certification" are often used interchangeably and this concept proposal is agnostic as to the precise nature of the proposed rules or the terminology.

[6] *See* About APEC, https://www.apec.org/About-Us/About-APEC (last visited Aug. 25, 2020); 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.

- Have cross-sectoral functionality both at the federal and state level if the sectoral approach to privacy regulation continues in the U.S.;

- Be based on voluntary participation and, as in the APEC CBPR, organizations would be certified by third parties that their privacy practices align with the code and thus are in compliance with the privacy laws of states that recognize the code;[7]

- Serve as a blueprint for future state laws and eventually for a comprehensive federal privacy law;

- Function as a safe harbor for compliance;

- Non-compliance with the code after certification would be a violation of section 5 of the Federal Trade Commission (FTC) Act's prohibition on unfair or deceptive acts or practices,[8] or of an equivalent state law provision or Unfair and Deceptive Acts and Practices (UDAP) statute;

- Good-faith efforts to comply with the code or certification could serve as a mitigating factor in enforcement by demonstrating that the certified organization has implemented a compliance program;

- Organizations would develop their privacy programs and practices with reference to the code, although some state-specific add-on requirements may still have to be considered and operationalized separately outside of the code;

- Through their oversight, complaint-handling and front-line enforcement functions vis a vis participating organizations, participating certification and monitoring bodies would ease the enforcement burdens on State AGs, state data protection authorities, the FTC and other relevant sectoral regulators or enforcement authorities; and

- Enable companies to leverage their compliance with the code to obtain certification under other similar international mechanisms for cross-border transfer or compliance purposes, such as the CBPR or the upcoming General Data Protection Regulation (GDPR) certifications and codes of conduct. Compliance with the code might even function as an "additional safeguard" for companies transferring data to the U.S. on the basis of standard contractual clauses in the wake of the Court of Justice of the European Union's recent decision which invalidated the EU-U.S. Privacy Shield.[9]

---

[7] An alternative approach to consider would be self-certification, as was the case for US companies certifying to the former EU-U.S. Privacy Shield.
[8] 15 U.S.C. Sec. 45(a).
[9] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems ("Schrems II"), July 16, 2020, available at http://curia.europa.eu/juris/document/document_print.jsf?docid=228677&text=&dir=&doclang=EN&part=1&occ=first&mode=lst&pageIndex=0&cid=9710274.

III. General Benefits of Codes of Conduct/Certifications

The features and objectives of the interstate privacy interoperability code listed above align with the following general benefits of codes of conduct and certifications for consumers, organizations and regulators:

- Facilitate organizational compliance with applicable legal requirements;
- Increase organizational accountability above and beyond compliance, to build more trust in the digital economy;
- Demonstrate to consumers, business partners and regulators that organizations' privacy practices have been reviewed by third parties and create an enforceable representation;
- Provide additional layers of oversight and enforcement by approved third-party certifiers, enabling enforcement or regulatory bodies with otherwise limited investigative and enforcement resources to leverage certifying bodies' review and monitoring of organizations' compliance with the code;
- Help small and medium-size enterprises (SMEs), which often do not have the necessary internal legal and compliance resources, to translate legal requirements into operational and scalable compliance steps. In effect, the code would serve as a ready-made privacy compliance program for organizations that do not have the resources and expertise to develop their own;
- Serve as a due diligence and risk management tool in procurement for companies seeking to identify accountable service providers, vendors and third-party processors; and
- Enable companies to leverage their compliance with one code or certification for compliance with another similar code or certification with overlapping requirements.

IV. Models for a US Interoperability Code

Codes of conduct and certifications are already used in the U.S. and throughout the world as both privacy compliance tools and cross-border data transfer mechanisms. In the U.S., the Children's Online Privacy Protection Act (COPPA) contains a safe harbor provision that allows for third parties to certify that an organization's privacy protections are "the same or greater" than what COPPA requires, the result of which is that the organization is deemed to be in compliance with COPPA.[10] In addition to COPPA, there are a number of examples from which to draw to formulate a multi-state interoperability code.[11]

A. APEC CBPR

[10] 15 U.S.C. Sec. 6503; and Federal Trade Commission COPPA Safe Harbor Program, https://www.ftc.gov/safe-harbor-program.

[11] In addition to the codes of conduct and certifications mentioned in this paper, data protection laws in Argentina, Brazil, Colombia, Panama, Mexico, Peru, Uruguay, Trinidad and Tobago, Singapore, The Philippines, South Korea, Dubai and Australia all enable codes of conduct or certifications in some form.

The U.S. already participates in the APEC CBPR and thus the CBPR may be the ideal model for the proposed multi-state code and certification. The APEC CBPR are a comprehensive privacy certification of organizations' privacy compliance programs. They enable certified organizations to transfer personal data across borders where such transfers would otherwise be prohibited by applicable privacy laws in participating APEC member economies.[12] The CBPR intend to ensure accountable cross-border data flows in the APEC region by requiring that privacy protections flow with the data. Specifically, a CBPR certification attests that an organization's privacy program complies with detailed requirements developed by the 21 APEC member economies to implement and operationalize the nine high-level APEC Privacy Principles in the APEC Privacy Framework, and that organizations also impose the same requirements on any third parties receiving their data.[13] The APEC privacy principles that must be operationalized in the CBPR program include: preventing harm; notice; collection limitation; uses of personal information; choice; integrity of personal information; security safeguards; access and correction; and accountability.

The U.S. was instrumental in developing the CBPR and was the first APEC economy to join the system in 2012. Each participating country must have at least one formally approved third-party certification body, known as an "accountability agent." Accountability agents review companies' privacy programs for compliance with the CBPR and certify such compliance, subject to annual review and recertification. While certification is voluntary, the CBPR become binding and enforceable on organizations once they are certified. As such, each participating APEC economy must also have a privacy enforcement authority that provides backstop enforcement, such as the FTC in the U.S. And each of these authorities must participate in the APEC Cross-border Privacy Enforcement Arrangement (CPEA), which sets out an enforcement cooperation framework for these authorities.[14]

As noted, while the CBPR were developed for the cross-border context, they also are a comprehensive privacy program that enables companies to achieve and demonstrate compliance with national privacy regimes regardless of whether data is transferred across borders.

Critically, the CBPR's objective of harmonization of privacy protections among APEC economies is analogous to the objective of a U.S. interstate interoperability code. In that respect, it is instructive that the recent United States-Mexico-Canada Agreement (USMCA), which replaced the North American Free Trade Agreement (NAFTA), both recognizes the APEC CBPR system as a valid data transfer mechanism and encourages "mechanisms to promote compatibility" between the three countries' privacy regimes. For the same reasons CBPR make sense internationally, they also make sense as the model for a harmonization and interoperability tool between U.S. states. Finally, U.S. businesses are becoming familiar with CBPR. Of all the companies who have obtained certification

---

[12] APEC refers to its members as "economies" because "the APEC cooperative process is predominantly concerned with trade and economic issues, with members engaging with one another as economic entities." The 21 APEC member economies are: Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Philippines, Russia, Singapore, Chinese Taipei, Thailand, The United States and Vietnam. *See* About APEC, https://www.apec.org/About-Us/About-APEC (last visited Aug. 25, 2020).

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

[14] In 2015, APEC added a second mechanism, the Privacy Recognition for Processors ("PRP").[14] It certifies a data processor's ability to provide data processing services to controllers at the level required by the CBPR and/or the controller.

under CBPR, the vast majority are based in the U.S.[15] Because CBPR are already formally recognized and accepted in the U.S. and promote compatibility between different jurisdictions, a U.S. interoperability code would fit well into the overall U.S. privacy schema.[16]

B. EU-U.S. Privacy Shield

The EU-U.S. Privacy Shield demonstrates another way that certifications and codes of conduct can function. While the Privacy Shield was recently held to be invalid as a data transfer mechanism by the Court of Justice of the European Union,[17] the substantive privacy requirements were not challenged or invalidated and thus remain a relevant and instructive source for a proposed U.S. interoperability code's substantive requirements. The primary difference between the Privacy Shield and certifications under the GDPR and APEC CBPR is that instead of using a third party certification body, the Privacy Shield allowed companies to self-certify that they were in compliance with the requirements. Self-certification, which required both a commitment to the U.S. Department of Commerce and a public commitment that an organization will abide by the principles, allowed organizations to transfer personal data of EU residents to the U.S. A Privacy Shield self-certification is enforceable[18] by the FTC under its Section 5 authority over unfair and deceptive practices.

C. GDPR

Articles 40-43 of the GDPR also enable codes of conduct and certifications. They can be used to demonstrate compliance with the GDPR in the same way we envision that a U.S. interoperability code can demonstrate compliance with state (or federal) law requirements. While the GDPR codes and certifications have not yet been finalized, they may become informative as to how a U.S. interoperability code might be designed and put to use. Alternatively, given the slow pace at which the GDPR codes and certifications are being developed, an interstate interoperability code could provide an opportunity for the U.S. to take a leadership role on privacy certifications and codes of conduct and serve as a potential model for GDPR codes and certifications.

The GDPR approach to establishing certification and monitoring bodies may also be instructive for any equivalent U.S. process. Based on that model, it might be appropriate to make the FTC responsible for accrediting certification or monitoring bodies in collaboration with state AGs (or other relevant regulatory or enforcement agencies), and those certification or monitoring bodies would be responsible for ensuring that an organization's privacy practices meet the requirements of the code.

---

[15] For a list of CBPR certified companies, see CBPR System Directory at http://cbprs.org/compliance-directory/cbpr-system/.

[16] *See* CIPL white paper on What Does the USMCA Mean for a Federal Privacy Law?, January 17, 2020, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_what_does_the_usmca_mean_for_a_us_federal_privacy_law__01.17.2020__4_.pdf.

[17] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems, July 16, 2020, available at http://curia.europa.eu/juris/document/document_print.jsf?docid=228677&text=&dir=&doclang=EN&part=1&occ=first&mode=lst&pageIndex=0&cid=9710274.

[18] Privacy Shield certifications are still enforceable with respect to data transferred while the Shield was in effect.

V. NEXT STEPS

A. DEVELOPING THE CODE

The first step towards developing the code would involve convening a working group comprising interested stakeholders including relevant state and federal officials.

This group could draw the substantive requirements of the code from a number of sources: (1) existing state law requirements,[19] (2) the CBPR program requirements; (3) the now-defunct Privacy Shield (as the substantive provisions were not challenged and reflect a set of GDPR-compliant rules; (4) the GDPR; (5) the Uniform Law Commissions draft model state law; (6) other significant pending comprehensive federal and state privacy bills and proposals; and (7) the International Organization for Standardization's (ISO) standards for privacy information management.[20] In addition, elements of the NIST Privacy Framework[21] could also potentially be integrated into the code in some capacity.

Of course, the stakeholders involved in drafting the code would be able to include additional elements as necessary, with the ultimate goal being a coherent, comprehensive and modern privacy program that could both serve as a code of conduct/certification and as a template for future state laws or a federal law.

B. KEY QUESTIONS ON PROCESS, GOVERNANCE AND OPERATION

The multi-stakeholder group will need to determine how exactly the code of conduct and certifications will function. They will need to address specifically the following questions:

- Will the code use third party certifications or self-certification?
- If it uses third party certifiers or monitoring bodies, how will those organizations be chosen and accredited?
- What governmental entities will provide oversight over the accreditation of such certifiers or monitoring bodies?
- What governmental entities will provide oversight for the certification process?
- How will the certification process function?
- What will be the legal impact of certification (e.g., will it be a "safe harbor")?
- Will participation in the code/certification serve as a mitigating factor in enforcement?

---

[19] Currently, only California, Maine and Nevada have data privacy laws, and both Maine's and Nevada's laws are very limited in scope. California is expected to place the California Privacy Rights Act on its general election ballot this November, which, if passed, would amend and update the California Consumer Privacy Act (CCPA) with a new set of privacy requirements that could be informative for a code. Several other states could also pass privacy laws later this year or next year, as state legislatures come back into session.

[20] International Organization for Standardization, ISO/IEC 27701, available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en.

[21] National Institute of Standards and Technology, NIST Privacy Framework, https://www.nist.gov/privacy-framework.

- How often will companies need to be recertified?
- How often will certifiers or monitoring bodies need to be re-accredited?
- How will the certifications be enforced?
- How will compliance with the code be monitored?
- How will additional state law requirements that are not covered by the code be handled?
- Will there be bridging mechanisms available in participating states so that certified companies have a process to certify state-specific additional requirements?

Existing laws and frameworks provide potential solutions to all of these questions, but it will be for the stakeholders to determine the path forward.

C. Obtaining Federal and State Recognition of the Code

Once the code has been drafted and the process, governance and operational features have been finalized, both the federal government and states will need to acknowledge that the code is effective in their jurisdictions. This may require the passage of legislation in some circumstances. Specific state privacy laws or a new federal privacy law could recognize and incorporate the code.

If you would like to discuss any of the comments in this paper or require additional information, please contact Markus Heyder, mheyder@huntonAK.com; Sam Grogan, sgrogan@huntonAK.com; or Matthew Starr, mstarr@huntonAK.com.