MEMO

To: Interested Parties
From: Information Technology Industry Council (ITI)
Re: Global Privacy Outlook for 2021

Privacy and trust are central to every company’s business and global operations. Since the EU’s General Data Protection Regulation (GDPR) became effective in May 2018, the GDPR has continued to have significant impact globally by providing a comprehensive privacy framework and inspiring legislation in various jurisdictions, including the U.S, Brazil, India, China, and elsewhere. Although protecting individual rights is essential for businesses across all sectors, the current landscape of privacy and data protection laws around the globe is increasingly complex and challenging to navigate, and the resulting fragmented regulatory approach could undermine data innovation practices, invariably limiting consumer choice and individuals’ welfare. In 2021, we will continue to see developments across the world on privacy and data protection. Below, we offer an ITI global privacy outlook with key issues to watch in various strategic markets.

United States
Federal Privacy Legislation

Despite a number of comprehensive privacy bills introduced by key Members of the committees of jurisdiction in the last Congress, there was little legislative progress, impeded by partisan disagreement over key issues including preemption and private rights of action. While control of the Senate shifted to the Democratic Party in January 2021, it is a mere 50-50 split with a tiebreaking vote from Vice President Kamala Harris. In practical terms, absent eliminating the filibuster, this means any privacy bill must attract significant bipartisan support to pass the Senate with 60 votes. However, the cast of Republicans and Democrats in the chair and ranking roles of both the Senate and House Commerce Committees remain largely the same and, while ITI expects a similar number of privacy bills to be introduced in the 117th Congress, it remains unclear how the parties will break the partisan logjams in either Chamber. We remain hopeful, however, that bipartisan talks will yield a framework that embraces consumers’ and policymakers’ desire for greater privacy protections that advance individuals’ data control rights and clearly define the responsibilities of companies using personal data while also recognizing the importance of data to the innovations that transform people’s lives and advance the public interest. ITI’s FAIR Privacy Framework offers one such roadmap.

Europe
Schrems II

The Court of Justice of the European Union (CJEU) released the judgement in the so-called Schrems II case that invalidated the EU-U.S. Privacy Shield in July 2020. While Standard Contractual Clauses (SCCs) remained valid following the decision, recent developments have cast doubt on the continuing reliability of this mechanism. In the post-Schrems II era, securing cross-border data transfers through the use of SCCs is crucial for all stakeholders and a reasonable, practical set of supplementary measures can help advance this goal. Although the U.S. and Europe have officially launched a bilateral negotiation for an enhanced Privacy Shield Agreement, the progress of the parallel UK-EU negotiation of an “adequacy” agreement and the transition to the new Biden-Harris Administration will impact the ultimate timeline of a deal. Given the ruling’s significant
impact on trade and global economy, industries across the world, including tech, continue to raise concerns, write letters and prepare comments.

In ITI’s recent submissions to two consultations on SCC reform post-Schrems II, we welcomed the European Commission’s focus on pursuing a risk-based approach as reflected in the GDPR and suggested stronger alignment with the European Data Protection Board (EDPB), who had offered guidance on the use of so-called “supplementary measures” for international transfers pursuant to SCCs. In particular, some aspects of the EDPB recommendations appear to go far beyond the requirements of the Schrems II ruling, depart from the GDPR’s risk-based approach, and propose a prescriptive use of supplementary measures or safeguards. These aspects of the recommendations could pose serious obstacles to international transfers personal data without necessarily benefitting the data protection of European citizens. In 2021, ITI views that both progress in the short- and long-term to stabilize international data transfers post-Schrems II are important to watch. In the short-term, we expect the negotiations on a successor to EU-US Privacy Shield will continue to move forward in parallel with the UK-EU adequacy negotiations. In the long-term, making progress at the OECD to build consensus on policy principles for trusted government access to private sector data can help lay the groundwork for a more durable multilateral solution.

e-Privacy Regulation

To complement the EU’s landmark personal data protection law, GDPR, and to fill gaps that the GDPR left with regards to electronic communication data, the EU proposed the e-Privacy Directive in 2017. The proposal would replace the old e-Privacy Directive and regulate how electronic communication service providers need to handle communication data produced through technologies such as instant messengers or voice-over-IP services. While the European Parliament agreed on its approach to the proposal rather quickly, the Council of EU Member States has spent years deliberating a compromise approach. Significant issues remain regarding provisions for further processing of meta data, among others. Our industry has repeatedly called for clarifications in this regard and alignment of the proposed e-Privacy Regulation with the GDPR’s risk-based approach so as not to disrupt many tech companies’ business models. A new proposal by the Portuguese Council Presidency might now resolve the gridlock and an agreement between Member States is seen as possible by March 2021. The agreement would then launch trilogue negotiations with the European Parliament and the European Commission. ITI sent a letter with comments on the Portuguese Council Presidency’s compromise text calling for greater alignment between GDPR and e-Privacy rules to avoid conflicting legal requirements.

e-Evidence Proposal

The European Commission published proposals to reform rules around law enforcement access to data in criminal investigations in April 2018. The e-evidence proposal seeks to introduce increased obligations for service providers to grant law enforcement access to data in cross-border criminal investigations. The Council of EU Member States published its position in November 2018 and the European Parliament’s, under the lead of the Civil Liberties, Justice and Home Affairs Committee (LIBE), recently published its negotiation mandate. Many EU countries are keen on extending law enforcement authorities’ abilities to gather data to support criminal proceedings and will thereby likely try to limit service providers’ ability to challenge government access requests on grounds of suspected fundamental rights abuses. Trilateral talks among the Council of EU Member States, the European Parliament and the European Commission will begin with a first meeting scheduled for 10 February 2021. In 2021, negotiations between the Council of Member States and the European Parliament will be crucial to watch, as the e-evidence file is likely to bear great significance in the European debate around
surveillance practices of governments and law enforcement access to data more broadly.

**Asia**

**China Personal Information Protection Law (PIPL)**

The Chinese National People’s Congress (NPC) released the long-awaited draft of the Personal Information Protection Law in November 2020, marking progress for China’s year-long effort towards a comprehensive privacy regime, as well as shaping the global privacy landscape. However, the Chinese approach on data localization and security requirements continues to be a potential hurdle for cross-border data transfers with the rest of the world. In our blog, we noted the Chinese draft law has many similarities with the European GDPR but includes unique Chinese characteristics, such as the lack of distinction for obligations on controllers/processors, data localization measures reflected through security assessment and certification requirements, and a potential exclusion of overseas organizations for national security violations. In 2021, it is important to watch how the draft law will interact with the other existing and proposed legal frameworks in China governing the protection of data related to critical infrastructure, including the Cybersecurity Law and the proposed Data Security Law.

**India Personal Data Protection Bill (PDPB)**

The Indian Parliament is set to introduce its privacy bill – called the Personal Data Protection (PDP) Bill – for full Parliamentary review during the first quarter of 2021. The Bill has been under review by a Joint Parliamentary Committee for over a year, but this committee is due to submit its report to the Parliament imminently. The Bill is the product of a multi-year process of consultation beginning with the creation of an expert committee to review India’s privacy protection scheme. The draft Bill loosely mirrors the European approach; however, the PDP Bill contains many additional troubling elements as highlighted in ITI’s comments, including: data localization for certain types of personal data even when the conditions for cross-border transfer are met; open government access to non-personal data; challenging notice and consent requirements; imbuing the government with the power to exempt its own agencies; and more. Despite the proposed amendments, the Bill is expected to be passed without significant changes to its major elements. The final Bill’s approach to data localization will likely influence India’s stance on data localization across sectors in future regulations. Many lawmakers have been vocal about localizing data storage for better sovereign access, even though it may have compatibility issues with similar regulations in other geographies. It’s possible that the final bill will be opened for additional comments from stakeholders with regards the absence/presence of judicial oversight for all kinds of data access requests from government.

**India Non-Personal Data Report (NPD)**

The quasi-government Expert Committee on Non-Personal Data (NPD) – established in 2019 – published its second version of the NPD Report at the end of 2020. This new Report outlines a regulatory framework that would force private entities to share NPD they possess with government and third-party entities that would create High-Value Data (HVD) sets. This draft is up for public comments until the end of January 2021, after which another draft is expected. The new Report has removed, refined, and further explained many aspects of the original report. For example, ITI believes that the removal of requirements to share data between private entities, the examination of intellectual property rights (IPR) protection, and the effort to establish a clearer line between the pending PDP Bill and the NPD framework are all positive steps. However, data localization requirements for certain categories of non-personal data, outstanding issues regarding the interplay of the PDP Bill and the NPD framework are all positive steps. However, data localization requirements for certain categories of non-personal data, outstanding issues regarding the interplay of the PDP Bill and the NPD framework are all positive steps. However, data localization requirements for certain categories of non-personal data, outstanding issues regarding the interplay of the PDP Bill and the NPD framework are all positive steps. However, data localization requirements for certain categories of non-personal data, outstanding issues regarding the interplay of the PDP Bill and the NPD framework are all positive steps. However, data localization requirements for certain categories of non-personal data, outstanding issues regarding the interplay of the PDP Bill and the NPD framework are all positive steps. However, data localization requirements for certain categories of non-personal data, outstanding issues regarding the interplay of the PDP Bill and the NPD framework are all positive steps.
“purpose,” among other elements, continue to be a cause of concern. The new Report retains the original concepts of community data ownership and economic rights which continue to be ambiguous and poorly defined. After providing comments to the first Report, ITI plans to submit comments to the second draft to ensure that the resulting Report and regulations, if any, are crafted in a way that would benefit the Indian economy to the greatest extent possible.

**Australia Privacy Act**

The Australian Attorney-General’s Department (AGD) recently opened a review of Australia’s Privacy Act of 1988 to consider whether the scope of the current law and its enforcement mechanisms remain fit for purpose. The review will likely bring the Australian privacy regime more in line with the EU’s GDPR in holding companies liable for the improper use of data. One vital area in which the Australian regime differs from GDPR is the former’s lack of controller/processor distinction, which would determine responsibilities for protecting the privacy of data subjects to ensure they have one single point of contact for exercising their rights. Other areas of the Privacy Act under consideration during the review are: the definition of personal information; protections for de-identified, anonymized, or pseudonymized information; notification; and the introduction of a statutory tort or direct right of action. ITI provided comments in November on an issues paper released by the AGD. The Australian government is planning to release a discussion paper in 2021 to seek further feedback on preliminary outcomes and possible reforms.

**Canada Consumer Privacy Protection Act (CCPA)**

On November 17, 2020, Canadian Innovation Minister Bains introduced Bill C-11, which proposes to replace Canada’s 20+ year old Personal Information Protection and Electronic Documents Act (PIPEDA) with a new Consumer Privacy Protection Act (CPPA). The proposed law has a number of characteristics that resemble GDPR, representing an attempt to bring Canada closer aligned with other economies’ privacy laws with an eye toward attaining an EU adequacy determination. The proposed legislation contains a number of important changes including establishing a set of transparency obligations for AI, algorithms, and other automated decision-making; providing guidance for new certification proposals for codes of practice; imposing strong sanctions for serious violations of the bill; and establishing a Personal Information and Data Protection Tribunal to oversee sanctions and enforcement. The bill is likely to move in the first half of 2021, once the government is able to form a coalition in the Parliament, and is expected to pass with few if any amendments. The legislation will enter into force 12-18 months after final approval. ITI has been tracking Canada’s various efforts seeking to update their privacy law, and we submitted comments to consultations on privacy and consent as well as privacy and AI. In 2021, it will be crucial to monitor how the Canadian Office of the Privacy Counsellor advances this initiative.

**Americas**

**Brazil LGPD**

The Brazilian General Data Protection Law (LGPD) went into effect on September 18, 2020. While the LGPD is similar to the GDPR, there are some notable differences, including the LGPD’s greater flexibility in legal bases for processing, more flexibility in opt-in and consent for processing, and broader allowances for international data transfers. The Brazilian Data Protection Authority (ANDP) was recently formed and is now beginning to draft the implementing regulations for the LGPD. As the ANDP forms its implementation plan and staffs up its team, it is essential to watch whether ANDP will provide more guidance in key areas, such as international data transfers, legal basis for processing, data subjects’ rights, and risk-based approaches. Additionally, monitoring enforcement actions will be crucial for companies to understand how the LGPD will work in practice.

The Brazilian Data Protection Authority (ANDP) recently opened a review of Australia’s Privacy Act of 1988 to consider whether the scope of the current law and its enforcement mechanisms remain fit for purpose. The review will likely bring the Australian privacy regime more in line with the EU’s GDPR in holding companies liable for the improper use of data. One vital area in which the Australian regime differs from GDPR is the former’s lack of controller/processor distinction, which would determine responsibilities for protecting the privacy of data subjects to ensure they have one single point of contact for exercising their rights. Other areas of the Privacy Act under consideration during the review are: the definition of personal information; protections for de-identified, anonymized, or pseudonymized information; notification; and the introduction of a statutory tort or direct right of action. ITI provided comments in November on an issues paper released by the AGD. The Australian government is planning to release a discussion paper in 2021 to seek further feedback on preliminary outcomes and possible reforms.

**Americas**

**Brazil LGPD**

The Brazilian General Data Protection Law (LGPD) went into effect on September 18, 2020. While the LGPD is similar to the GDPR, there are some notable differences, including the LGPD’s greater flexibility in legal bases for processing, more flexibility in opt-in and consent for processing, and broader allowances for international data transfers. The Brazilian Data Protection Authority (ANDP) was recently formed and is now beginning to draft the implementing regulations for the LGPD. As the ANDP forms its implementation plan and staffs up its team, it is essential to watch whether ANDP will provide more guidance in key areas, such as international data transfers, legal basis for processing, data subjects’ rights, and risk-based approaches. Additionally, monitoring enforcement actions will be crucial for companies to understand how the LGPD will work in practice.