COMMENTS OF THE AMERICAN BAR ASSOCIATION
SECTIONS OF ANTITRUST LAW AND INTERNATIONAL LAW
ON THE WHITE PAPER ON A DATA PROTECTION FRAMEWORK FOR INDIA

January 31, 2018

The views stated in these Comments are presented on behalf of the American Bar Association Sections of Antitrust Law and International Law. They have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and therefore may not be construed as representing the policy of the American Bar Association.

I. Introduction

The Sections of Antitrust Law and International Law (“the Sections”) of the American Bar Association respectfully submit these comments on the White Paper of the Committee of Experts and the Ministry of Electronics and Information Technology (the “MEITY”) on a Data Protection Framework for India (the “White Paper”). As noted in the White Paper, the Committee of Experts was set up by the Government of India “to study various issues relating to data protection in India, make specific suggestions on principles underlying a data protection bill and draft such a bill.” The objective is to “ensure growth of the digital economy while keeping personal data of citizens secure and protected.”

The White Paper looks to “International Practices” in discussing the various issues. These comments are intended to further this dialogue and reflect the Sections’ experience in international and cross-border privacy and data security issues. Although we are not experts in the law of India, the Sections’ long involvement in these issues rests on the participation of both private and public sector lawyers, economists, and market participants, reflecting the interests of all those who engage in, benefit from, and enforce legal rights relating to, digital as well as traditional commerce in which personal data plays an important role. The Sections do not advocate on behalf of any particular interest or party; rather, we offer our comments as constructive input of the type invited by the Committee of Experts.

The Sections commend the Committee of Experts for presenting a comprehensive, thoughtful analysis that takes into account the vast technological changes and legal developments in the global data marketplace. The Sections also commend the Committee of Experts for seeking consistency with international data protection laws while taking into account the needs and goals of India “to harness the benefits of the digital economy and mitigate the harms consequent to it.” In these Comments, the Sections make several suggestions that we believe both further the goals of modernization and harmonization and serve the desired balance between individual privacy and the development of information markets and services that benefit Indian nationals and the development of a global marketplace.

---

1 White Paper at i.
II. Executive Summary

The Sections’ comments make the following suggestions:

• **Jurisdiction**: The Sections believe that adopting the longstanding approach to extraterritoriality contained in the 1995 Data Protection Directive and the current EU Directive on Privacy and Electronic Communications ("E-Privacy Directive") is a sound solution. These approaches, where consistently applied, have served to encourage the predictability of domestic privacy and data protection regulations around the world. If the General Data Protection Regulation ("GDPR") approach is adopted; however, we suggest that the limitations on the test imposed both by the recitals and by EU common law be reflected in the text of the Indian data protection law to ensure that India does not adopt an approach that, as a practical matter, is more stringent than the EU approach.

• **Definitions of Personal Data**:
  
  o The Sections support the White Paper’s tentative conclusion to apply the GDPR’s definition of “personal data,” but suggest that the concept of “reasonable linking” be applied in addition to the GDPR’s definition.
  
  o The Sections also suggest that the concept of “reasonable efforts” to define whether data has been anonymised or pseudonomised be included in these concepts, and the law in India recognize that a contractual prohibition on a private party re-identifying anonymised data should be considered in determining whether re-identification is reasonable.
  
  o As to the definition of “sensitive data,” the key for India, in the Sections’ view, will be to determine appropriate areas that are sensitive in the life of Indian data subjects and base a definition on those elements.

• **Cybersecurity and Breach Notification**: As an alternative to an immediate reporting mandate, language that requires controllers to report security incidents “without unreasonable delay” will help to ensure that competent bodies receive prompt notice, while providing controllers with sufficient time to conduct a proper review of the security incident and mitigate any potential threats to the data subjects. Such an approach also will limit instances in which information provided to the competent body is either inaccurate or incomplete, and help to ensure that notice provided to the competent bodies is accurate and meaningful.

• **Cross-Border Data Transfers and Data Localization**: Lowering barriers to data transfers across national borders play a critical role in the development of innovative technologies and digital goods and services, as well as contributing to the growth of the broader economy. Data transfer and related data localization requirements are not necessary for, and are indeed unrelated to, privacy protection or security concerns. Instead they raise barriers to entry for cross-border competitors. In reality, the security of data depends on the administrative, physical, and technical safeguards that are put in place to protect the confidentiality, integrity, and availability of the data.

• **Consent/Notice/“Legitimate Interest”**: In lieu of the legitimate interest standard, the White Paper suggests a residuary ground or, as an alternative, that the data protection authority designate certain activities as lawful, and provide guidelines for data controllers. The Sections note that a data protection authority “carve out” for certain data processing activities may lack
the flexibility of the “legitimate interests” basis, while still placing a burden on data controllers, with a significant and disproportionate impact on smaller data controllers. Regardless of the approach, the Sections encourage the data protection authority to provide guidance on the grounds for data processing generally to ensure that data controllers can process personal data efficiently and for the benefit of consumers.

- The Sections suggest that it would be prudent to incorporate a privacy impact assessment into the law to help organizations comply with data protection obligations, including the effectiveness of notice. The Sections also recommend that the appropriate regulator provide guidelines, recommendations, and best practices on a privacy impact assessment, as well as whether and when it is mandatory for data controllers.

- If a data trust score is assigned, consumers or an independent self-regulatory body should be responsible for providing the data trust score. This approach would likely reduce compliance costs and promote transparency with resulting benefit to consumers.

- A consent dashboard may be feasible assuming the compliance costs are minimal, fair, and proportional to the data controllers’ size and revenue.

- **Automated Decision Making**: As an initial matter, the Sections urge that disclosure of the logic behind automated decisions should be subject to the protection of intellectual property rights so as to protect the ability of businesses to innovate and compete. In the Sections’ view, the appropriate balanced and workable approach is that taken by the Article 29 Working Party in its recently adopted Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, including the materiality limitation.

- **The Right to be Forgotten**: A principle-based approach would provide a vehicle for balancing individuals’ interest in limiting permanent use of their data with the legitimate needs of those to whom they provided their data in the first place.

- **Accountability/Fines**:
  - **Civil Liability Standard**: The Sections recommend the application of a negligence standard and recommends that any standard that is adopted be narrowly circumscribed and limited to data processing activities that are likely to cause actual, material harm to the individual and include appropriate exceptions.
  - **Insurance**: The Sections view it as unnecessary and overly burdensome to require by law that data controllers take out insurance policies to meet their potential liabilities under the data protection law.
  - **Penalties**: The Sections recommend that penalties be effective, proportionate, and have a deterrent effect. Linking penalties to a high percentage of total worldwide turnover of the defaulting data controller in the preceding year could be disproportionate and excessively punitive. The Sections recommend that the data protection framework for India provide discretion to the adjudicating authority to determine when a fine is appropriate and, if so, what amount should be assessed. In addition, the Sections recommend that civil penalties should increase according to the relative seriousness of the violation, similar to the gradated manner in which fines are assessed under the GDPR model, with appropriate considerations of whether the full penalty is appropriate for a particular potential violation.
We appreciate the opportunity to provide commentary to the Committee of Experts and the MEITY, and would be pleased to continue our participation or respond to any comments or inquiries that may be useful during this process.

III. Specific Suggestions

1. Jurisdiction: Extraterritorial Application of the Law

The White Paper appropriately asks about the scope of extraterritorial application of the new data protection law. In particular, the paper asks “[t]o what extent should the law be applicable outside the territory of India in cases where data of Indian residents is processed by entities who do not have any presence in India?” This is an issue of keen importance to U.S. entities, and one that the GDPR has resolved in a manner that may be viewed as controversial. In the Sections’ view, the key issues are to ensure that the law permits companies to predict whether it will apply to them, and to ensure that its application is consistent with general principles of international jurisdiction.

The GDPR extended the territorial reach of EU privacy law in new ways. Specifically, it provides that the obligations of EU privacy law extend to entities outside of the EU if those entities: (1) offer goods or services to data subjects in the EU; or (2) “monitor the behaviour” of those data subjects. The concept of “monitoring the behaviour” of data subjects is meant, according to the draft Regulation’s recitals, to encompass online behavioral advertising or other activities commonly undertaken to compile information on data subjects.

The second element of the GDPR’s extraterritorial reach is a significant expansion of current EU data protection law. Under the existing 1995 EU Data Protection Directive, entities operating outside of the EU would be subject to the application of EU law only if they are either established within an EU Member State or they use equipment (particularly servers) located in the EU to collect information on EU data subjects. In addition, the E-Privacy Directive, which currently is also being renegotiated among the European institutions, has taken a more flexible position. Article 3(1) of the E-Privacy Directive provides that it “shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.” The approaches set out in the EU Data Protection Directive and the E-Privacy Directive have permitted non-EU and multinational companies to structure their behavior appropriately in light of the jurisdictional requirements of European data protection law, and have led to a predictable and workable approach. The new provisions of the GDPR may lead to differing results in practice.

To the extent that India follows the GDPR approach, however, it is important to recognize that both the recitals to the GDPR and longstanding principles of European common law place important limitations on the scope of its jurisdictional tests. Adopting only the specific tests in the GDPR without recognizing these limitations could result in India adopting a far more expansive jurisdictional stance than may be intended.

---

3 Regulation 2016/679, art. 3(2), 2016 O.J. (L 119) 1, 32-33.
4 See EU Data Protection Directive 95/46/EC, art. 4(1).
“Offering Good or Services.” In respect of the first prong concerning parties offering services in the EU, recital 23 of the GDPR contains a useful clarification:

In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller’s, processor’s or an intermediary’s website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.6

Accordingly, the mere accessibility from the EU of a company’s website or the use of a certain language are not sufficient to trigger jurisdiction under the GDPR. The targeting of EU users must be more obvious and “envisioned,” for example, by allowing them to order goods and having them shipped to the EU, by using the Euro as a currency option, or by offering content in languages adapted to EU users.

These principles sound in EU common law. In the Pammer case,7 the Court of Justice of the EU (“CJEU”) was asked to clarify when an Internet service can be considered to target a Member State. The CJEU held that mere accessibility of a website does not suffice. Similarly, the indication of the trader’s address, e-mail address or phone number (without international code) cannot be construed as targeting. To the contrary, the CJEU highlighted the following examples of activities that can demonstrate an intention to target:

- the express mentioning that the service is provided to users in a Member State;
- paying search engines to have its website favorably indexed in order to facilitate access by consumers in particular Member States;
- the international nature of the services;
- the provision of international telephone numbers;
- the use of Internet domain levels other than those of where the service provider is established (or general ones, such as .eu, or .com); and
- the mentioning of international clientele, and accounts written by such customers.

“Monitoring the Behaviour.” The second trigger for the applicability of the GDPR is whether the party outside the EU “monitors the behavior” of users in the EU. On this prong, recital 24 of the GDPR provides as follows:

In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the Internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for

---

6 GDPR, recital 24.
analysing or predicting her or his personal preferences, behaviours and attitudes.

The recital assumes tracking of(295,304),(535,319)(253,316),(497,331) behavior that is quite extensive. The tracking should occur with the intention of influencing the user based on an analysis and prediction of personal preferences. Whether this description of “monitoring” would apply to generally accepted Internet advertising techniques is an open question. Current Internet advertising strategies rely on data that does not contain contact or identifying information of “natural persons,” but might rely on device identifiers, IP addresses, cookies, and other proxies for identifying a particular advertising subject on the Internet. It may be that “monitoring” that focuses on serving targeted advertising to a user based solely on device identifier, IP address, or other identifier that cannot be used to identify a “natural person” should not fall under the definition. It remains to be seen how the EU will interpret this provision of the GDPR.

In summary, the Sections believe that adopting the longstanding approach to extraterritoriality contained in the 1995 Data Protection Directive and the current E-Privacy Directive is a sound solution. These approaches, where consistently applied, have served to encourage the predictability of domestic privacy and data protection regulations around the world. If the GDPR approach is adopted, however, we suggest that the limitations on the test imposed both by the recitals and by EU common law be reflected in the text of the Indian data protection law to ensure that India does not adopt an approach that, as a practical matter, is more stringent than the EU approach.

2. Definitions of Personal Data

A key element of any data protection law is the definition of “personal data.” The White Paper provisionally proposes to define “personal data” as “data about/reating to an individual” and “data from which an individual is identified or identifiable/reasonably identifiable.” As the White Paper notes, the question of whether an individual may be reasonably identified “can be direct or indirect.” The White Paper asks whether the standard should refer to an individual who is “identified,” “identifiable,” or “reasonably identifiable” by the data in question. It also asks whether there should be a different level of protection for data that actually “identifies” a person, as compared to the situation where an individual may only be “identifiable” or “reasonably identifiable” by certain data.

Data may also be anonymised (that is, made so it no longer identifies an individual) or pseudonymised (referred to by a pseudonym that cannot be associated with an individual). The White Paper appropriately asks whether standards should be adopted for these protective processes, and whether the approach in the GDPR is the right standard for India to consider.


9 Recent EU cases may suggest that even general Internet advertising techniques that do not rely on the name or actual contact information of a particular Internet user might still be considered “monitoring” because of the broad definition of “personal information” favored by some European courts. In Google v. Vidal-Hall, [2015] EWCA (Civ) 311 (Eng.), a British court held that browser-generated information collected using cookies (such as Internet surfing habits and news reading habits) constitutes private or personal information.

**Definition of “personal data.”** Privacy laws in different jurisdictions take somewhat different approaches to defining “personal information.” In the EU, personal data means any data relating to an identified or identifiable natural person. In the U.S., “personal data” is data that can be “reasonably linked” to a specific individual.\(^{11}\) In Singapore, “personal data” refers to data about an individual who can be identified from that data. The GDPR defines “personal data” as follows:

‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The definitions provided in both the Data Protection Directive and the GDPR imply that any data capable of being associated with an identifiable person will constitute personal data.

The GDPR approach is a sensible one that recognizes that data should be defined as “personal data” only if that person “can be identified” by that data. The U.S. definition puts an important gloss on the GDPR’s concept—data should be considered “personal” to an individual only if it can be “reasonably linked” to that person. In other words, an identifier that cannot be reverse-engineered or otherwise linked to an individual should not be considered to be “personal information” as to that individual.

Further, data held by a company that could, in theory, be used to identify an individual if combined with other data to which the company does not have access also should not be considered “personal data” as to that company and that individual because the company does not have access to the “key” that could connect the data to the individual. For these reasons, we support the White Paper’s tentative conclusion to apply the GDPR’s definition of “personal data,” but suggest that the concept of “reasonable linking” be applied in addition to the GDPR’s definition.

**Anonymisation/Pseudonomisation.** Anonymous or pseudonymous data appropriately falls outside of the definition of “personal information” because such data can no longer reasonably identify a particular individual. Anonymization implies any procedure whereby data may no longer be directly or indirectly associated with “an individual,” provided that the individual in question cannot be re-identified through reasonable efforts. The challenge is how to define the standard of “reasonable efforts” used to re-identify an identifiable individual. The GDPR suggests that “account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments” (GDPR, recital 26), which may be an effective model. In the U.S., the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule provides two methods for de-identifying personal data (the Expert Determination Method and the Safe Harbor method), which have proven to be effective in protecting personal data.\(^{12}\) Contractual or other limitations on the re-identification of anonymized data also could be considered as limitations on the ability to re-identify anonymised data.


\(^{12}\) See 45 C.F.R. §§ 164.514(b)(1) and 164.514(b)(2); see also “De-identified Health Information,” in Department of Health & Human Services, *Summary of the HIPAA Privacy Rule*, available at https://www.hhs.gov/hipaa/professionals/privacy/laws-regulations/index.html.
We suggest that the concept of “reasonable efforts” to define whether data has been anonymised or pseudonomised be included in these concepts, and the law in India recognize that a contractual prohibition on a private party re-identifying anonymised data should be considered in determining whether re-identification is reasonable.

**Sensitive Personal Information.** As the White Paper recognizes, virtually all data protection regimes define some level of “sensitive” personal information, based on societal views of personal data that would be particularly harmful for data subjects if disclosed inappropriately. Generally, the category of “sensitive” personal information requires a higher degree of consent prior to its collection and processing by a data controller.

Definitions of “sensitive” personal information vary by jurisdiction because this term depends upon societal views of sensitivity that vary from country to country. The EU GDPR definition focuses on personal data that reveals “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership . . . genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.” In the United States, the Federal Trade Commission (“FTC”) “defines as sensitive, at a minimum, data about children, financial and health information, Social Security numbers, and certain geolocation data.” These definitions largely overlap, although the United States does not generally protect as “sensitive” data about union membership, political opinions, religious beliefs, or ethnic origin.

The key for India, in the Sections’ view, will be to determine appropriate areas that are sensitive in the life of Indian data subjects and base a definition on those elements. This inquiry can, of course, be informed by the experiences of other countries, but in the end must be a uniquely Indian solution. The U.S. definitions, which have been based on specific cases, are generally based on predictions of actual harm if information is compromised—lost financial information can lead to economic loss or identity theft; lost health information can lead to disclosures that could be harmful to data subjects; lost information about children could subject them to risk; highly specific geolocation information could be used by bad actors. We suggest that this general fact-based approach, based on predictions of actual harm, be considered by the drafters of the data protection law.

3. **Cybersecurity and Breach Notification**

Given the increasing frequency of data breaches in modern life, the White Paper appropriately focuses on a national standard for data-breach notification. It tentatively concludes that individuals should be notified of a breach of their personal information where it is likely that these individuals will suffer privacy harms as a consequence of the breach. The White Paper also suggests that the relevant data protection authority (“DPA”) or other regulator should be notified “immediately” about data breaches, and that the DPA may issue codes of practice that specify the formats for such notifications. The White Paper notes that fixing too short a time for individual notifications may be onerous for small businesses, and may prove to be counterproductive because the organization may not have reliable information about the breach and its likely consequences in too short a period of time.

As data breaches continue to grow in magnitude and complexity, the Sections acknowledge that timely and accurate information regarding a breach is an essential part of protecting data subjects from harm, allowing parties to take swift measures to secure sensitive information, and prevent further harm.

---

13 GDPR, art. 9(1).
from taking place. As the White Paper recognizes, it is important that the competent body is promptly aware of new and evolving threats.

The United States has had data-breach notification standards as a matter of state law for almost 15 years, and has significant experience with notification, both to affected consumers and to regulators. The Sections commend the White Paper for recognizing that so-called “immediate” notification schemes can be counterproductive, because the scope of a typical data breach affecting thousands or millions of data records cannot be known “immediately.” In our experience, the standard adopted by the GDPR of requiring notification to regulators within 72 hours of discovery is likely to be ineffective because so little information can be known about a complex breach within such a short period. The United States data breach notification laws require notification “without unreasonable delay,” and some specify a goal of 45, 60 or 90 days after a breach is discovered. The United States notification laws also provide exceptions for notification in the event of a request by law enforcement or, in most cases, when no harm is likely to result or when data was encrypted. In practice, “immediate” notice requirements can result in premature notice before the scope and extent of a breach can be fully known, which may not benefit consumers or regulators.

Under an immediate notice regime, a controller that becomes aware of a security incident inevitably will focus its initial attention and resources on complying with its notice obligations. Given the proposed rigid timing requirement, the controller may feel compelled to conduct an expedited review and initially gather only enough information sufficient to provide notice. Such notice may occur before the controller has obtained an accurate and complete understanding of the root cause and the scope of the incident, which the controller will need before it can contain the incident and adequately secure the affected systems and data. This would be particularly true in instances where a forensic investigator is required to investigate the incident. The result is that personal data may remain vulnerable to further unauthorized access while the controller is focused on providing immediate notice to the competent body.

An immediate notice requirement also may result in excessive reporting to competent bodies. As an example, a controller that provides immediate notice to a competent body based on an expedited review of the security incident subsequently may determine that the incident is not a reportable event because no personal data was in fact compromised. Such over-reporting would place a strain on the resources of competent bodies, and would make it difficult for competent bodies to accurately determine whether prompt notification to data subjects is warranted. Over time, competent bodies would find it increasingly difficult to evaluate root causes of true reportable events and identify security incident trends that may justify closer monitoring or allocation of resources. Authorities’ resources would be strained managing events in which data were not actually compromised. And data subjects could experience reporting fatigue, rendering them unable to differentiate high- and low-risk threats.\textsuperscript{15}

As an alternative to an immediate reporting mandate, the Sections believe that language that requires controllers to report security incidents “without unreasonable delay” would help to ensure that competent bodies receive prompt notice, while providing controllers with sufficient time to conduct a proper review of the security incident and mitigate any potential threats to the data subjects. Such an approach also will limit instances in which information provided to the competent body is either inaccurate or incomplete, and help to ensure that notice provided to the competent bodies is accurate and meaningful.

In addition, we commend the White Paper’s focus on potential harm as a trigger to notification obligations. To further clarify, however, the Sections recommend including that the risk of damage should be “material.” Like the immediate notice regime, lack of materiality can lead to excessive reporting to competent bodies, adding further unnecessary burdens and expense for all parties.

4. Cross-Border Data Transfers and Data Localization

Under the current technological landscape, data are being transferred internationally on a daily basis. Automated processes in global enterprises have become a critical component to effectively and efficiently run cross-border operations. Global businesses that automate their processes likely transfer data across borders on a daily basis.

**Cross Border Data Transfers:** The Committee of Experts discusses two tests for cross-border transfers, the adequacy test and the comparable level of protection test for personal data. It provisionally recommends adoption of the adequacy test to be administered by a proactive data protection authority, noting that it is “particularly beneficial because it will ensure a smooth two-way flow of information, critical to a digital economy.”

This provisional view appears to adopt the GDPR model without explicit endorsement of the various other mechanisms by which data can be transferred from the EU, including binding corporate rules, standard contractual clauses, and frameworks such as Privacy Shield.

We would note, first, that there are at least three, not two, models for international data transfer. The third model is to allow the free flow of personal information based on the express or implied consent of the data subject. This is the model that has been adopted by many countries with innovative high technology entities and start-ups including the United States.

Second, the adequacy test does not “ensure a smooth two-way flow of information, critical to a digital economy.” Only a few countries have been deemed adequate by the EU, excluding most key non-EU markets. Even if India explicitly includes the various other mechanisms adopted by the EU, the adequacy rule engenders more uncertainty than a smooth flow of data. The disruption caused by the CJEU invalidating the US-EU Safe Harbor framework, effective immediately upon entry, was well documented. The current legal challenge to the EU Standard Contractual Clauses relied upon by most entities transferring data out of Europe creates similar uncertainty. The cost, time and resources for filing under Binding Corporate Rules (BCRs), which cover only intra-group data transfers, also make such options unreasonable to many large companies even in a market as large as the EU; as a result, relatively few companies have successfully filed for BCRs. The costs and uncertainty may impact business decisions to do business in India. Supporting the seamless cross-border flow of information will continue to ensure India’s presence in the global economy.

A third mechanism in the current EU-US data protection framework discussed in the White Paper, is Privacy Shield. Utilizing this mechanism, enterprises can self-certify compliance with more stringent data protection requirements. This solution provides increased flexibility for the data

---

16 White Paper, part II, Chapter 8.3 Provisional View, p. 68.
17 The countries are set out in the White Paper at p. 64.
processors and enforceable legal obligations that protect the data subject’s privacy. The new Privacy Shield requires clearer safeguards from U.S. authorities and contains a dedicated ombudsman to follow up on complaints or other inquiries from data subjects. Even this mechanism is subject to uncertainty in light of its review by the Article 29 Working Group.\textsuperscript{20} The Sections once again stress the importance of having a self-regulation procedure to achieve compliance with applicable data privacy laws while increasing operational efficiency, especially given the increase in cloud-computing.

\textbf{Data localization}: The Committee of Experts adopts the provisional view that “India will have to carefully balance the enforcement benefits of data localisation with the costs involved pursuant to such requirement. Different types of data will have to be treated differently, given their significance for enforcement and industry. It appears that a one-size fits-all model may not be the most appropriate. Thus, while data localisation may be considered in certain sensitive sectors, it may not be advisable to prescribe it across the board.”

Lowering barriers to data transfers across national borders plays a critical role in the development of innovative technologies and digital goods and services, as well as contributing to the growth of the broader economy. Data localisation requires data operators to use facilities (server(s)/data center(s)) located in-country either owned or provided by third parties; the Sections believe that backing up a database that is primarily stored elsewhere is not an acceptable compliance solution. Data localisation requirements are not necessary for, and are indeed unrelated to, privacy protection or security concerns. Instead they raise barriers to entry for cross-border competitors. There is no empirical evidence to our knowledge that supports the proposition that segmenting database architecture by the nationality of the data subjects provides greater data security than databases that house data from multiple nationalities. In reality, the security of data depends on the administrative, physical, and technical safeguards that are put in place to protect the confidentiality, integrity, and availability of the data. Where the data stored is not as important as how the data is stored and which safeguards protect it.

The economic costs are significant. At a minimum, data localisation forces companies to spend more resources on local server establishment. It also may impede or prevent the development of new capabilities, technologies, or services. The free flow of cross-border data allows both start-ups and established enterprises, including small and medium-sized enterprises (“SMEs”), to provide less costly and more efficient services. If localization restriction requirements were adopted, SMEs would be denied these benefits, and could become less efficient and competitive in the global marketplace. SMEs may not be able to enjoy the benefit of cloud technology in a network that is artificially fragmented by localization requirements.

In addition, requirements that certain data be stored locally may be impractical for businesses that operate using complex server architectures with interlocking data sets, such as social networks and other global service providers. Such restrictions threaten harm to consumers, competition, and innovation, with consequences to national and international economies. The effects could range from foreign investment flows to GDP growth and consumer welfare. The Sections believe that data localisation of personal data or persons engaged in business activities will reduce transparency and severely curtail the ability or interest of global companies considering doing business with Indian

\textsuperscript{20} Article 29 Data Protection Working Party, EU-U.S. Privacy Shield Report, Nov. 28, 2017, available at https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf. (the WP29 “identified a number of important unresolved issues” and “the WP29 calls upon the Commission and the U.S. competent authorities to restart discussions” and “an action plan has to be set up immediately...”).
companies, especially new and emerging Indian businesses which represent a key genesis of economic growth. Global companies will shift to more transparent and less risky economies.

5. Consent/Notice/“Legitimate Interest”

Modern data processing requirements in the European Union permit several grounds for lawful processing of data, including: (1) pursuant to the consent of the data subject; (2) when necessary to perform a contract with the data subject; (3) to comply with various legal obligations/provide the vital interests of a data subject; is in the public interest; or (4) is necessary for purposes of “legitimate interests.” The White Paper, in contrast, focuses more on requiring consent from the data subject prior to data processing. A strict reliance on consent as a basis for processing, however, can create issues. For example, true consent is undermined when consumers experience “consent fatigue” and simply check “accept” to move through a transaction or signup without meaningfully reviewing options before providing consent. For this reason, other bases for processing are often used. Implicit, or opt-out, consent is commonly used in online services and mobile applications. In the United States, the Federal Trade Commission (“FTC”) has recognized that consent reasonably may be inferred from the context in which the data subject interacts with the data controller, and that affirmative express consent should be required only when the particular use of data would be unexpected by the consumer. As the FTC noted, “[c]ompanies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction, or the company’s relationship with the consumer, or are required or specifically authorized by law.” This concept captures the need to obtain consent where a consumer would not expect the specific processing at issue, but recognizes that modern digital life includes circumstances in which the need to obtain written consent at every turn is a burden on consumers and businesses alike.

In lieu of the legitimate interest standard, the White Paper suggests a residuary ground or, as an alternative, that the data protection authority designate certain activities as lawful, and provide guidelines for data controllers. The Sections note that a data protection authority carve out for certain data processing activities may lack the flexibility of the “legitimate interests” basis, while still placing a burden on data controllers. The Sections believe that rejecting legitimate interest could negatively impact the online and mobile markets in critical ways. Specifically, the divergence in standards could result in compliance burdens that could have a significant and disproportionate impact on smaller data controllers. Regardless of the approach, the Sections encourage the data protection authority to provide guidance on the grounds for data processing generally to ensure that data controllers can process personal data efficiently and for the benefit of consumers.

How can data controllers be incentivized to develop effective notices?

Data controllers may be incentivized to develop effective notices through increased activity by industry trade groups, market leaders, consumers’ rights groups or others that may be in a position to encourage sound data privacy practices. Although law enforcement safe harbor and rulemaking are effective, the Sections encourage the data protection authority to also explore other non-enforcement measures that may relieve the burden on regulators and encourage market participants to bring value to consumers.

Would a consent dashboard be a feasible solution in order to allow individuals to easily gauge which data controllers have obtained their consent and where their personal data resides? Who would regulate the consent dashboard? Would it be maintained by a third party, or by a government entity?

The Sections note that a consent dashboard may be feasible assuming the compliance costs are minimal, fair, and proportional to the data controllers’ size and revenue. Setting aside the technical
challenges of incorporating a consent dashboard across industries and consumer platforms, the Sections note that the lead up to implementation of a third party or government entity maintained dashboard will pose challenges for enforcement. The Sections encourage data protection authorities to provide written guidance to anticipate challenges to government enforcement efforts and policy.

6. Automated Decision Making

*Is guaranteeing a right to access the logic behind automated decisions technically feasible? How should India approach this issue given the change associated with it?*

The Sections urge that any disclosure of the logic behind automated decisions should be subject to the protection of intellectual property rights so as to protect the ability of businesses to innovate and compete.

In the Sections’ view, a workable approach is that taken by the Article 29 Working Party in its recently adopted Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. The Guidelines provide that a controller making automated decisions must “tell the data subject that they are engaging in this type of activity; provide meaningful information about the logic involved; and explain the significance and envisaged consequences of the processing.” Accordingly, the right to access the logic behind automated decisions, even where technically complex, is guaranteed in a meaningful and understandable way for data subjects. The Sections also note that European Union, in the recently enacted GDPR, defines the universe of automated decision-making subject to its rule in Article 22(1) as “a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her” (emphasis added). The Sections suggest a materiality limitation in line with the GDPR approach and believes that adopting the transparency requirements identified in the Article 29 Working Party Automated Decisions guidelines is a sound solution.

7. The Right to be Forgotten

The Sections recognize and acknowledge the Committee’s desire to maintain individuals’ control over the continued use of their information by incorporating a “right to be forgotten” within a data protection framework for India. The Sections also appreciate the Committee’s recognition that a right to be forgotten should be balanced with the rights to freedom of speech and expression. However, data controllers have other legitimate and compelling reasons to retain personal data, a need we suggest should be balanced with an individual’s right to be forgotten.

The right to be forgotten, if adopted, should be implemented as a set of principles recognizing individuals’ ability to cause the deletion of their personal information from digital memory where appropriate, rather than as an overriding personal right that may conflict with the need of some data controllers to maintain that data in certain circumstances. Describing the right to be forgotten in overly broad terms could have unintended consequences, including:

---

21 For example, the GDPR identifies the following lawful purposes for further retention: “for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.” Regulation 2016/679, 2016 O.J. (L 119), recital 65.
• Denial of individual benefits (e.g., post-termination or retirement benefits administration could be hampered if a former employee has a virtually unilateral right to be forgotten with regard to human resources records).

• Denial of an individual’s ability to enforce legal rights (e.g., if a group of female employees believe they are unfairly compensated based on their gender, but a handful of female employees has invoked their right to be forgotten and their compensation and benefits records were deleted, then the group of women, the employer, and the courts may be denied the ability to accurately evaluate and resolve the claim).

• Facilitating illegal activity (e.g., in cases of fraud the victim may be unaware of the alleged crime and thus unable to request retention of relevant records in a timeframe suitable to pursue a claim, a problem exacerbated by the perpetrator’s conceivable ability to request erasure of records that may be relevant but that include personal data about the perpetrator).

• Endangering health and safety (e.g., in the case of clinical trials, an individual’s adverse reactions or other medical outcomes are of paramount importance to both the development of effective pharmaceuticals and other treatments and to the safety of persons participating in the trial).

• Impeding the advancement of legal defenses (e.g., business records very often include personal data and those records may be relevant to establishing legal compliance or mounting a legal defense; deletion of those records based on individuals’ privacy concerns may deprive a business of its ability to demonstrate compliance or to defend allegations of noncompliance, and similarly may deny authorities a full and fair view of the merits of a claim).

A principle-based approach would provide a vehicle for balancing individuals’ interest in limiting permanent use of their data with the legitimate needs of those to whom they provided their data in the first place. As with other principle-based obligations (such as those for data integrity, consent, and the like), the data controller would be provided clear guidance as to the conditions under which it may process or use personal information, but would not face the kind of absolute prescription that may not fully serve other, equally valid interests that demand (or even require) the retention of data.

8. Accountability/Fines
   a. Strict Liability

The Sections appreciate the Committee’s desire to incorporate strong principles of accountability into the data protection framework for India. However, the Sections are concerned that imposing strict liability for all breaches of a data controller’s obligations could result in the unfair imposition of liability even where a data controller has taken all reasonable measures under the law and established practices and standards. For example, under a strict liability regime, a data controller could be held liable for harms resulting from a security breach even if the data controller had implemented reasonable and appropriate administrative, technical, and physical safeguards to protect its information systems from malicious third parties or other foreseeable risks to individuals’ personal information.

The Sections recommend the application of a negligence standard that would require individuals to prove that the data controller did not act reasonably under the circumstances. We believe that the adoption of a negligence standard would permit individuals to recover damages for harm in appropriate circumstances, while at the same time ensuring that data controllers implement their data protection obligations in a reasonable and appropriate manner.

If the data protection framework in India ultimately incorporates any strict liability provisions, the Sections recommend that such provisions be narrowly circumscribed and limited to data processing
activities that are likely to cause actual, material harm to the individual. The Sections also recommend that any strict liability provisions be subject to appropriate exceptions, such as when the harm is caused by a force majeure act or the individual herself contributed to the harm.

b. Joint and Several Liability

The Sections also are concerned that imposing joint and several liability on all data controllers involved in processing personal information that ultimately causes harm to an individual is inappropriate because such a rule would conflict with underlying tort law concepts. Accordingly, joint and several liability would result in unjust treatment of innocent data transferors and transferees. In tort law, joint and several liability typically applies where there are two or more actors who both breach a duty of care to a third person, and either it cannot be determined which one caused the damage to the third person, or both caused the damage. Consistent with tort law, the GDPR includes only very narrow joint and several liability for data transferors and data transferees, limited to instances in which both caused damage to the individual.\(^{22}\)

The Sections recommend that the data protection framework for India exclude joint and several liability, or at least narrowly circumscribe its application to instances in which two or more parties both caused damage to the individual. The full application of joint and several liability would conflict with tort law concepts in several respects. First, when one party alone—be it the data transferor or the data transferee—breaches its duty to the individual, there is no justification for holding another party liable who breached no duty to the individual. Second, in the highly unlikely case that both data transferor and data transferee breached their duty to the individual, it is even less likely that the individual will not be able to determine which party caused the damage, or that both breaches will be inseparable causes of the damage. The inclusion of joint and several liability in the data protection framework for India could subject innocent parties to full liability for another party’s breach.

c. Insurance

The Sections view it as unnecessary and overly burdensome to require by law that data controllers take out insurance policies to meet their potential liabilities under the data protection law. Unlike other circumstances where compulsory insurance is generally required—such as automotive liability insurance or taxi insurance that aims to protect individuals from severe harm caused by uninsured motorists or undercapitalized companies that cannot be identified by the individual in advance—individuals can identify in advance the data controllers with whom they share their personal information and make an informed decision about whether to disclose such information to the data controller or not.

d. Penalties

The Sections recommend that penalties should be effective, proportionate, and have a deterrent effect. Linking penalties to a high percentage of total worldwide turnover of the defaulting data controller in the preceding year could be disproportionate and excessively punitive. Accordingly, such penalties could discourage companies from reporting potential violations or cooperating with regulators to solve problems, particularly in the data security area, or from choosing to do business or process data in India at all.

Even the GDPR, which provides for significant fines, has carefully calibrated criteria for determining when higher fines are appropriate and for determining the appropriate amount of the fine.

---

\(^{22}\) Regulation 2016/679, 2016 O.J. (L 119) at 81.
in each individual case. Accordingly, the Sections recommend that the data protection framework for India provide discretion to the adjudicating authority to determine when a fine is appropriate and, if so, what amount should be assessed. In addition, the Sections recommend that civil penalties should increase according to the relative seriousness of the violation, similar to the manner in which fines are assessed under the GDPR model, with appropriate considerations for whether the full penalty is appropriate for a particular potential violation.

IV. Conclusion

The Sections appreciate the opportunity to comment on the White Paper, and commend the Committee of Experts and the MEITY for this open and transparent process. If the Sections can clarify any of the matters discussed herein or answer any questions, we would be pleased to do so.

---

23 Id. at 82-83.