JOINT COMMENTS OF THE AMERICAN BAR ASSOCIATION’S SECTION OF ANTITRUST LAW AND SECTION OF INTERNATIONAL LAW ON THE EUROPEAN COMMISSION’S PUBLIC CONSULTATION ON BUILDING THE EUROPEAN DATA ECONOMY

April 26, 2017

The views stated in this submission are presented jointly on behalf of the Section of Antitrust Law and the Section of International Law (the “Sections”) of the American Bar Association (“ABA”) only. These comments have not been approved by the ABA House of Delegates or the ABA Board of Governors and, therefore, may not be construed as representing the policy of the American Bar Association.

Introduction

The Section of Antitrust Law and the Section of International Law (collectively, the “Sections”) of the American Bar Association welcome the opportunity to respond to the Public Consultation on Building the European Data Economy (“Consultation”) of the European Commission (“Commission”). These comments focus on two specific issues addressed in the Consultation: data localization requirements and access to raw machine-generated data. In brief, the Sections support the Commission’s efforts to resist data localization restrictions, as they hamper competition in digital markets. As regards proposals to mandate access to raw machine-generated data, the Sections encourage the Commission to rely on existing competition law and procedure to regulate access to raw machine-generated data effectively and to refrain from separately regulating such access, because of the risk that overbroad access requirements will chill innovation and investment.

Free Flow of Data

The Sections agree that lowering barriers to data transfers across national borders will 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. The Sections concur that ensuring a free flow of data among EU Member States is of significant and growing importance in building the single digital market. The Sections share and echo the Commission’s concern, however, about the effects, whether inside or outside the EU, of enacting data localization laws or rules that limit the storage, movement, or processing of data to specific geographies or jurisdictions.\(^2\) Such data localization restrictions could hamper the development of digital markets and impede the innovation that digitization makes possible. The Sections therefore welcome the opportunity to expand on the views expressed by the Commission.

**Potential Impact of Localization Requirements**

The protection of personal data and ensuring data security are often cited as reasons for imposing data localization requirements. The Sections agree that data security and privacy are important objectives. These objects, however, are already being addressed through EU data privacy legislation, whereas localization requirements may by unnecessary, or sometimes even unrelated to, privacy protection or security concerns. At the same time, data localization requirements can 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 Real Burden Created by Localization Requirements**

Unnecessary localization requirements may adversely affect not only multinational companies operating in various countries, but also nations, firms, or individual Internet users trading and communicating via the Internet. Data localization requirements can impair competition, for instance, by limiting access to, or artificially raising the price of, cheaper or more

---

innovative data services; forcing cross-border businesses to arrange duplicative and inefficient data storage and processing capabilities; inhibiting start-ups and subject matter experts from scaling up their activities, entering new markets, or centralizing data and analytics capacities; and hampering the adoption of cloud storage and computing.

At a minimum, data localization forces companies to spend more resources on local server establishment. It also may impede or prevent the development of new capabilities, technologies, or services. In particular, the free flow of cross-border data allows both start-ups and established enterprises to provide less costly and more efficient services, including small and medium-sized enterprises (“SMEs”). If localization restriction requirements were adopted by individual Member States generally, SMEs would be denied these benefits, and could become less efficient and competitive in the global marketplace. In particular, SMEs may not be able to enjoy the benefit of cloud technology in an EU network that is artificially fragmented by multiple 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, EU, and international economies. The effects could range from foreign investment flows to GDP growth and consumer welfare. Consumers could lose control over the portability of their data and the ability to choose between service providers.³ Localization restrictions would lead to fragmentation rather than better protection and are inconsistent with the objective of building efficient digital commerce, including an effective digital single market in the EU.

Recommended Approach for Evaluating Localization Requirements

The new General Data Protection Regulation,⁴ which becomes effective in May 2018, precludes EU Member States from establishing data localization requirements based on the protection of personal data. This restriction, however, likely would not constrain the imposition

of localization requirements on other bases. The Sections encourage the Commission to consider measures, which may be used in combination: a legislation requiring that any governmental data localization requirements within the EU satisfy objective and harmonized criteria to ensure that such requirements do not disproportionately impede competition in the EU; pending adoption of such a binding measure, publication of guidelines indicating the Commission’s views of non-privacy related criteria that could be used to justify data localization requirements and the limitations of such criteria; and enforcement actions by the Commission challenging data localization requirements that impermissibly restrict competition without objective justification.

The Sections respectfully submit that data localization requirements should be permitted only where they are demonstrably necessary to achieve a legitimate privacy and security objective that could not be achieved by less restrictive means. This framework would parallel the recognition of the free flow of goods and services, which is a key component of the EU single market. The Sections believe that there is no legal or economic justification for requiring personal data as a broad class of digital information to be stored in local servers without regard to the sensitivity of such data or the relative security of alternative storage solutions. Indeed, there is nothing inherently more secure about local storage versus regional or global solutions. The Sections respectfully suggest that alternative solutions will often satisfy the goals for which localization is proposed. For example, if a localization restriction is proposed to assure public accessibility and/or supervision of legal authorities, it would be worth exploring whether the objective could be achieved by closer and more effective cooperation between Member States rather than data localization restrictions. Common standards of data security protection, with appropriate oversight, should address concerns that are advanced in support of localization.

Second, the Sections respectfully suggest that data localization requirements should be applied principally to critical information infrastructure (“CII”) operators, defined based on bona fide, technology neutral criteria. Moreover, the Sections submit that not all personal data that CII operators collect should be subject to localization requirements. The Sections believe that this requirement should be limited to data that are critical to national security or the public interest and only when localization requirements are necessary to achieve the protections required. Accordingly, if the data have been anonymized by technical measures that cannot be reverse engineered, then such data should not be subject to localization requirements. In summary, the Sections believe that data localization restrictions are not necessarily required to provide adequate
protection for data. Furthermore, such restrictions may impair the development of the EU’s single digital market. Free flow of data is often critical to support technical innovation and the competitiveness of regional economies. We encourage the Commission to pursue measures to identify and dismantle unjustified barriers to data transfer and storage, including through appropriate infringement proceedings and, potentially, through legislation.

**Data Access and Transfer**

In the Communication, the Commission expresses concern that, although the “ever-increasing amounts of data...generated by machines or processes based on emerging technologies” “presents rich opportunities for players in the data market to innovate and apply insights into this data,” ⁵ “in some cases...market players holding data keep the data generated by their machines...for themselves, thus potentially restricting reuse in downstream markets.” ⁶ While there may be cases in which the refusal to license a data set could raise competition concerns, the Sections caution that these cases are likely to be rare, and we do not believe it is necessary to create a new substantive regulation to cover those potential cases. In the Sections’ view, in addition to being “sufficient to ensure fair and innovation-friendly results, facilitate easy access for new market entrants and avoid lock-in situations,” ⁷ existing competition law principles caution against the imposition of broad data access obligations. ⁸

Likewise, the United States Supreme Court long ago observed that, “[i]n the absence of any purpose to create or maintain a monopoly, [Sherman Act § 1] does not restrict the long-recognized right of trader or manufacturer engaged in an entirely private business, freely to exercise his own independent discretion as to parties with whom he will deal.” ⁹ Competition law

---

⁵ Communication at 8.
⁶ Id. at 9–10.
⁷ Id. at 10.
⁸ See also Margrethe Vestager, “Speech: Big Data and Competition,” Remarks delivered at EDPS-BEUC Conference on Big Data, Brussels, (Sept. 29 2016), available at https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/big-data-and-competition (noting that “the competition rules weren’t written with big data in mind. But the issues that concern us haven’t changed. We’re not here to get in the way of innovative ideas. If companies need to collect large sets of data, or share data with their rivals to build better products, we don’t object to that. As long as they don’t hurt consumers in the process, by undermining competition...I’m convinced we can make big data, not a threat, but the key to a better future.”)
in the United States has considered the appropriate balancing of these factors in developing the boundaries of duties to deal.\textsuperscript{10}

The skepticism that the United States Supreme Court has expressed about forced sharing stems from the same concerns acknowledged in the Commission Staff Working Document—namely, that imposing sharing obligations, including in the form of data portability requirements, “could have a chilling effect on firms’ incentives to innovate.”\textsuperscript{11} In the EU, the Commission and the European Courts also have extensive experience with situations in which companies with market power may be required to provide third parties access to an essential facility or input, and they have similarly imposed such requirements only under strictly limited conditions, for example in the European Court of Justice’s judgments in Microsoft,\textsuperscript{12} IMS,\textsuperscript{13} and Bronner.\textsuperscript{14}

In sum, the Sections endorse the use of competition law principles, which have been considered and developed over many years in the EU and internationally, to address competitive concerns relating to data access. Premature ex-ante regulation could chill investment and lead to suboptimal outcomes, particularly in light of the rapidly evolving nature of big data practices and the large investments that are being made in this area.

\textbf{Conclusion}

The Sections appreciate the opportunity to provide comments on the Commission’s Consultation on Building the European Data Economy. The Sections would be pleased to respond to any questions the Commission may have regarding these comments, or to provide any additional comments or information that may be of assistance to the Commission as it considers these issues.

\textsuperscript{11} STAFF WORKING DOCUMENT at 48.