关于民法典草案第3编第6章的意见

非常感谢有机会向全国人民代表大会提出我们对《民法典》修改草案中关于个人信息和数据隐私章节的意见。我们代表的企业来自各行各业，且与中国有着深厚长久的商业关系。许多单位都对中国的《网络安全法》、《电子商务法》和其他行业特定法规和标准中有关个人信息和数据隐私的条款非常关注，《民法典》修正草案第3编第6章也不例外。

此次《民法典》修订案的措辞看似旨在明确保护个人隐私及个人权利，但遗憾的是这也同时显现了一些关于个人隐私的保护和服务于客户利益的担忧。其中有些条款有悖于业内惯例及业界经验，从而可能降低数据保护的效率，进而削弱企业为中国顾客提供最好产品和服务的能力。

我们担心《民法典》中关于数据隐私的规定会和中国现行的一些网络安全问题解决方法一样，不仅有碍全球经济的进一步融合，还会造成世界经济更大的分离。在当今这个正值世界政治和社会风云变幻的时代，我们担忧这样的政策可能会加剧目前国际市场的不稳定情绪，有碍各国在全球贸易一体化及合作中获益。

我们恳请中国在制定个人信息和数据隐私相关政策时能更多地考虑全球的商业环境。我们认为制定的政策不仅应该能够推动市场竞争及透明度，也应当有针对性且非歧视。因此政策的制定应当更多地参考国际规范，例如经合组织隐私准则和亚太经合组织跨境隐私规则等，同时还要遵守中国对世贸组织的承诺。

我们一直秉承与中国政府通过合作的方式来共同解决行业合理关切的问题，支持并推进中国在安全、经济和社会方面目标的实现。为此我们提出以下建议：

隐私、隐私信息和个人信息的定义（第 811-813 条）

第 3 编第 6 章第 811-813 条阐述了几个关键术语（包括隐私、私人信息和个人信息）的定义和范围。虽然第 811 和 813 条对这些术语给出了简要的解释和示例，但这些定义仍然模糊。例如，在没有明确解释 “个人信息” 和“私人信息”区别的情况下，很难区分“个人信息”和“私人信息”。因此，我们建议全国人民代表大会更明确地定义这些术语的范围以及它们之间的关系。

个人信息收集（第 814 条）

草案要求所有组织在收集、使用自然人个人信息时要征得被收集者同意。但是处理数据如果以征求同意为基础，会为商业活动带来不必要的障碍。我们认为应该设立一系列的个人信息处理机制。要求所有种类的数据都征求同意会使数据主体不堪重负且使问题复杂化。

此外，《民法典》要求组织明示收集和使用信息的目的；允许自然人“依法查阅、抄录、或复制”其个人信息，并允许自然人在特定情况下提起请求及时删除其个人信息。

我们建议就“信息持有人有义务允许个人请求删除其个人信息”提出更明确的界定。特别是，为与全球规范相符，已经匿名化的或根据法律要求保留的个人信息应不受这条要求的约束。我们建议任何匿名化的个人信息都不应被视为个人信息，或者采用一种更基于风险考虑的方法，即当个人提出要求删除其个人信息时，应适当考虑其可行性，信息持有人可被要求在可行的情况下， 在一定时间内采取合理步骤删除相关的非匿名化个人信息。

第 814 条要求公司明示收集、使用信息的目的，此规定措辞含糊，没有考虑到消费者数据分析以及获取被征集者同意未来使用其数据的复杂性。企业通常无法预测从消费者数据中获得的信息会如何推动随后数据的使用并由此改善产品和服务。太笼统地要求企业告知个人未来使用其信息的特别目的，会

限制企业利用数据造福中国消费者的能力。例如，企业会因此无法利用顾客信息来为顾客定制新产品以满足顾客还未被满足的需求或解决安全问题。

当企业分析数据的目的是提供更好、更创新的服务时，顾客会因此受益。公司可以通过把收集的信息匿名化，并对接触信息的企业人员作出限制的方式来遵守保护顾客隐私标准的规定，同时又可通过交叉使用数据来创新服务回报顾客。

个人查阅收集的信息（第 815 条）

第 815 条要求公司提供渠道，允许自然人依法查阅、抄录、或复制其个人信息，并在特定情况下，自然人可以请求及时更正或删除其个人信息。

我们担心“允许个人依法查阅收集的信息”这一规定是否具有可操作性。草案没有就企业需要保存哪些数据供个人查阅以及需要为此保留多长时间作出规定。我们建议草案在这些方面作出更明确的说明。此外，我们还想指出的一点是，数据有时是可做匿名化处理并添加到数据集合中的。鉴于很难提取匿名数据供个人查阅，因此如果个人可以随时要求查阅其数据会严重制约企业使用匿名化数据的能力，从而对个人信息的保护造成更大的风险。在数据保留时间方面，我们注意到中国的金融服务监管机构已经设立了记录保存期限。如果有必要立法，我们建议行业监管机构有权根据行业情况设定合适的保留期限，以避免因为数据保留期限的不一致导致的不必要的费用支出。

更改和分享个人信息（第 817 条）

第 817 条要求信息收集人、持有人不得泄露、篡改、毁损其收集、存储的个人信息;未经被收集者同意,不得向他人提供个人信息。

我们建议就该条规定中的下列措辞提供更明确的解释：“篡改”一词的意图以及向他人提供个人信息时“征求被收集者同意”的方法。因为该措辞可以解读为：在向第三方服务供应商提供个人信息之前需要征得同意。该规定可能会限制经济活动和增长。“不得篡改个人信息”及“不得向潜在第三方提

供个人信息”的规定可能会限制各单位进行研发、分析和创新，采取安全措施以及开发更符合顾客需求的新产品的能力。

惩罚和责任（第 816 条）

本条列出了行为人不承担民事责任的五种情形，但是并没有指出行为人在违反规定后应该受到什么惩罚以及该承担怎样的民事责任。

我们期望明确实施惩罚的措施和责任。我们建议，惩罚虽然能够起到威慑的作用，但是不能极端到严重制约经济增长或鼓励轻率诉讼。

告知个人（第 817 条）

本条规定在发生或者可能发生个人信息泄露、毁损、丢失的情况时，信息收集人、持有人应当及时采取补救措施并告知被收集者。

此条规定措辞过于宽泛，要求在未造成实质风险的情况下（例如泄露姓名和地址等不太敏感的信息时），就需告知信息被收集者。我们建议明确风险界限，可以限制造成实质性风险的情况所发生的次数和频率。过于宽泛的措辞可能会导致监管机构及个人接受过量的信息泄露提示，这样既不能保护个人免受实质威胁，也不能给监管机构或相关个人提供有用信息。

要求公司明示数据收集目的的措辞含糊不清，没有考虑到消费者数据分析的复杂性。这个规定会制约企业利用数据造福中国消费者的能力。例如，企业会因此而无法利用顾客信息来为顾客定制新产品去对应顾客的未满足需求。当企业分析数据的目的是提供更好、更创新的服务时，顾客会因此受益。企业可以通过把收集的信息匿名化，并对接触信息的企业人员作出限制的方式来遵守保护顾客隐私标准的规定，同时又可交叉使用数据进行创新服务去回报顾客。此外，我们建议中国人民代表大会允许将收集的数据用于匹配目的。

感谢全国人民代表大会给我们机会就《民典法》草案发表意见。我们希望这些意见能够在全国人民代表大会和司法部法制办公室审查《民典法》草案时

发挥建设性的积极作用。我们会持续关注并希望有机会就这些问题进一步对话。

署名：
中国美国商会
上海美国商会
中国华南美国商会
美国人寿保险协会
美国保险协会
服务业联盟
美国商会
美中贸易全国委员会

2018 年 11 月 3 日

November 3, 2018

Comments on Part 3, Chapter 6 of the Draft Civil Code

Thank you for the opportunity to share with the National People's Congress our comments on certain draft updates to the Civil Code regarding personal information and data privacy protection. Our organizations represent companies across a wide range of industries, with deep, long-standing commercial ties with China. Many of us have shared concerns over provisions regarding personal information and data privacy in China's Cybersecurity Law, Ecommerce Law, and other sector-specific regulations [and standards], and we have some similar concerns with regard to the draft amendments to the Civil Code at Part 3, Chapter 6.

This new draft language in the Civil Code appears intended to carve out explicit protections for personal privacy and individual rights, but regrettably presents concerns over the protection of personal privacy and for the service of consumer interests. Some of these provisions do not align with established and proven industry best practices, and could result in less effective protection of data, while also impeding companies' ability to deliver the best products and services to Chinese consumers.

Our organizations are concerned that this approach to data privacy, like aspects of China's current approach to other cybersecurity issues, is leading to greater separation between the economies of the world rather than global economic integration. At a time of significant political and social change globally, we are concerned that such policies may exacerbate troubling trends in markets around the world that move countries away from the benefits of integrated and cooperative global trade.

We respectfully urge that China's policies regarding personal information and data privacy be better aligned to reflect the globalized commercial environment. These policies should be crafted to advance market competition and promote transparency. They should be narrowly tailored and non-discriminatory, taking into account international norms, such as the OECD Privacy Guidelines and the APEC Cross Border Privacy Rules, and they should also comply with China's World Trade Organization commitments.

We remain committed to working with the Chinese government to find solutions that address the legitimate concerns of industry in ways that support and enhance China's security, economic, and social goals. With that in mind, we share the following:

Definitions of Privacy, Private Information, and Personal Information (Article 811-813)
Articles 811-813 set forth the definition and scope of several critical terms—including privacy, private information, and personal information—used in part 3 chapter 6. Although articles 811 and 813 provide a brief explanation and some examples, these terms remain unclear. For instance, it is challenging to delineate "personal information" from "private information" without a clear explanation as to their differences. Therefore, we recommend NPC more clearly define the scope of these terms and their relation to each other.

Collection of Personal Information (Article 814)
The draft text would require that all organizations obtain consent for the collection and use of personal information of natural persons. Using consent as the only basis for processing data will create unnecessary barriers for commerce. There should be a range of processing mechanisms for personal information. Requiring consent for all types of data will unduly complicate and overwhelm data subjects.

In addition, the Civil Code requires organizations to explicitly indicate the purpose of the data collection and usage; permit an individual to "inspect, copy, or reproduce" their personal information; and allow an individual to request deletion of his or her personal information in specific circumstances.

We propose that more clarity be provided around an organization's obligation to permit an individual to request deletion of his or her personal information. In particular, consistent with global norms, personal information that is already anonymized, or required by law to be retained should be exempt from this requirement. We would propose that any anonymized personal information should not be considered as personal information, or a more risk-based approach be adopted, with due consideration for feasibility, whereby an organization could be required to take reasonable steps to delete relevant, non-anonymized personal information where feasible and within a reasonable time period upon request by an individual.

The draft language in Article 814 requiring companies to explicitly indicate the purpose and usage of their data collection is vague and does not account for the complexities of generating insights from consumer data and gathering consent for the future uses of data. Companies frequently cannot anticipate how initial insights gleaned from consumer data might drive subsequent use of that data for the development of enhanced products and services. Overbroad requirements to inform individuals of the specific future uses of their information could hamstring companies' ability to utilize data to the benefit of Chinese consumers. For example, it could prevent companies from using customer information to tailor new products aimed at addressing customers' unmet needs or addressing security concerns.

Consumers benefit when companies analyze data sets for the purpose of creating better and more innovative services. Companies can observe strict privacy standards to protect consumers by anonymizing collected data and restricting who within an organization has access to it, while at the same time using it cross-functionally to support innovations responsive to consumers.

Individual Inspection of Collected Data (Article 815)

Article 815 would require that companies provide a channel through which an individual can "inspect, copy, or reproduce" their personal information, and must allow an individual to request changes to or deletion of their personal information in specific circumstances.

We are concerned about the practicalities of the requirements allowing for individual inspection of collected data. The draft language does not stipulate what data companies must keep on file for users to track and see, or for how long they must retain it for this purpose. We propose that more clarity be provided here. We also would like to note that data is sometimes anonymized and added to data sets. Given the difficulties of extracting anonymized data for an individual's inspection, if an individual can at any time demand access to such data, the use of anonymized data may be severely circumscribed, resulting in greater risk to the protection of personal information. As for the data retention period, we note that China's financial services supervisory bodies have already established records retention periods. If legislation is necessary, we would recommend that industry supervisors be given the authority to set industry-suited retention periods to avoid any inconsistency and unnecessary expenses related to data retention.

Changing and Sharing Personal Information (Article 817)

The draft language would require that the information collector and holder not "tamper" with personal information and shall not provide personal information to others without the consent of the individual.

We propose that more clarity be provided around the intent of the word "tamper" and the method of "consent" that is required to share personal information with others, as this language could be interpreted to require consent before sharing personal information with third party service providers. Such requirements could restrict economic activity and growth. Organizations could be restricted from performing research and development, analytics, and innovation, taking security precautions, and could be impeded from creating new products that better address their customers' needs because of these anti-tampering and potential third-party sharing restrictions.

Penalties and Liability (Article 816)

The draft would outline five scenarios where an actor may not bear civil liability. However, it does not provide any guidance on what penalties and civil liability may be imposed for violations.

We anticipate that more clarity will be provided around the imposition of penalties and liability. In the interim, we propose that while penalties should serve as a deterrent, they should not be so extreme as to severely restrict economic growth or encourage frivolous litigation.

Notice to Individuals (Article 817)
The draft would provide that in the event of the occurrence or possible occurrence of personal information disclosure, damage, or loss, remedial measures be taken promptly and the recipient be informed.

This language is overbroad and could require notification to individuals of incidents that do not pose a meaningful risk, such as the disclosure of less sensitive information like name and address. We recommend that this provision be clarified to include a harm threshold that helps limit the number and frequency of events to only those that pose a meaningful risk. Overbroad language runs the risk of inundating regulators and individuals with notices of breach, which neither protects individuals from real threats nor provides regulators or affected individuals with useful information.

Language requiring that companies explicitly indicate the purpose of data collection is vague and does not account for the complexities of generating insights from consumer data. This threatens to hamstring companies' ability to utilize data to the benefit of consumers. It could, for example, prevent companies from using customer information to tailor new products aimed at addressing customers' unmet needs. Consumers benefit when companies analyze data sets for the purpose of creating better and more innovative services. Companies can observe strict privacy standards to protect consumers by anonymizing collected data and restricting who within an organization has access to it, while at the same time using it cross-functionally to support innovations responsive to consumers' needs. Moreover, our organizations recommend that NPC allow secondary purposes of data that are compatible with the initial collection.

We thank the National People's Congress for providing this opportunity to comment on the draft regulations. We hope that these comments are constructive and useful to the National People's Congress and the Legislative Affairs Office of the Ministry of Justice as they review the draft Civil Code. We would appreciate the opportunity for further dialogue on these issues and are happy to follow up as appropriate.

Signed,

The American Chamber of Commerce in China
The American Chamber of Commerce in Shanghai
The American Chamber of Commerce in South China
The American Council of Life Insurers

American Insurance Association
Coalition of Services Industries
US Chamber of Commerce
US-China Business Council