THE US-CHINA BUSINESS COUNCIL
美 中 贸 易 全 国 委 员 会

优化互联互通：关于改善中国信息技术环境的最新建议

2018 年 2 月

自 2017 年 6 月《中华人民共和国网络安全法》生效以来，中国政府已经实施了一系列网络安全法规，对在华经营的外国公司和本土公司产生了广泛的影响。

美中贸易全国委员会 2017 年中国商业环境调查报告显示，82%的会员公司对中国处理信息流动和技术安全的方式表示关切。这主要是因为这些新的网络安全政策影响了它们开展日常业务的能力。中国在投资、数据输出、产品安全评估和关键信息基础设施领域的政策，以在其他市场并未出现的方式影响着在华的外国公司和本土公司的运营。这些政策限制企业采用全球最佳实践的能力，使其无法完全采用既高效又受全球认证的安全技术防护措施。这些政策也使企业难以互相交流处理安全隐患的信息，致使消费者和企业均处于不太安全的环境之中。

我委员会所提建议旨在解决企业在中国使用信息技术时遇到的具体问题。我委员会对多家企业的技术人员展开了广泛的访谈，提出了以下建议，并为平衡运营和安全需求提出了可行的方案，旨在有效且有建设性地解决中国政府和企业共同关切的问题。我委员会非常感谢能够有机会提出这些建议，并希望就这些问题与相关主管部门展开进一步的讨论。

挑战一： 数据流动与本地化

中国的数据政策阻扰了企业在华设施与其其他全球业务之间的通信，抑制了跨境创新，并因为要求重复安装信息技术基础设施而增加了企业的成本。这些政策也影响了中国“互联网+”和国家大数据战略等发展规划的实施。 这些限制性政策影响了外国公司和本土公司在中国运营全球性平台、开展电子商务以及进行尖端科研活动的能力。

企业技术高管在接受采访时表示，中国的数据流动和本地化政策给大数据分析的使用造成了困难，影响了产品支持、安全和创新。例如：

- 在中国运营风力发电机组的能源公司需就机组群的运作状况与全球总部保持持续的沟通，使其全球团队能够应对停电并预防其他事故的发生。
- 生产“智能制造”设施中使用的高科技、互联网连接设备的公司需要访问设备中的数据，以便其提供远程维护和维修服务。
- 出售用于基础设施开发所需的工业用车的公司需要访问车辆的遥测和性能数据，以便为其客户提供关于机器性能及预防性维护等方面的信息。

- 金融服务公司需要分析跨境数据以预测消费趋势，为客户提供有针对性的服务，并识别潜在的非法交易。

过于严苛的数据管理制度阻碍以上及其他重要的运营活动，损害企业及其客户的权益。

在多数情况下，关于数据流动的规定旨在维护公民个人信息和其他重要数据的安全。然而实际上，要求数据本地化，进行跨境数据流动安全审查，或是使用中国国内的技术，这对实现上述目标收效甚微。保护数据隐私最有效的国际标准应由行业主体共同制定，采用全球最佳实践，并且对数据的存储位置或传输的地点未做更多要求。网络安全专家认为，发生网络攻击最常见的原因在于系统保护不够、错误操作和部分用户的疏忽大意。仅选择在中国拥有基础设施的服务提供商，而非受全球认证的有保护隐私和安全实践的服务提供商，会导致个人信息和重要数据的安全性最终更有可能遭到侵害。

无法将全球性网络与中国境内的网络连接起来也会带来安全风险。本地的软件或本地的供应商在使用全球技术时可能无法排除产生的故障或就故障进行有效的沟通。当维护问题、技术问题或犯罪性网络侵入发生时，无法联通全球通信网络致使公司无法快速做出应对。

确保跨境数据的自由流动是创新数字经济的重要组成部分，创新数字经济的发展已被中国列为首要的任务之一。“十三五”规划、“中国制造 2025”和“互联网+”等规划强调发展智能技术和互联网技术，中国高层政府官员也强调在中国境内和在 20 国集团的框架下拥有开放性、互联性网络的重要意义。

为促进开放性并确保数据安全，中国应参考跨国公司提供的最佳实践和专业知识。这些知识将传统商业实践和全球信息网络结合起来，是在制定全球标准的过程中发展出来的。允许企业、支持团队和互动性产品在全球范围内访问相关信息是“智能技术”的关键组成部分。“智能技术”是中国“十三五”规划的目标之一，也是“互联网+”、促进大数据发展行动纲要等跨领域高层次政策规划，以及通过智慧城市提高能效的发展规划，和中国金融业的发展规划能够成功实施的必要条件。

几点建议

- 中国应缩小国家安全和“国家秘密”的定义范围，以确保企业不会无意中违反关于存储和传输这类信息的规定。该定义的范围应仅限于对国家安全有直接影响的信息。

- 中国应指明，只有原始个人信息和“重要数据”才必须在中国进行本土化存储。中国也应允许数据副本被送到国外进行分析和处理，以确保运营效率，鼓励大数据创新。这将在保留对数据的地域管辖权的同时，仍然允许企业开展重要的业务。中国也应明确表述并确认，只有关键信息基础设施运营商收集的个人信息和重要数据才需要进行数据本地化以及数据输出安全审查，应免除对网络运营商在上述方面的要求。

- 中国应确认“默认同意”是出境数据传输的一个充分标准。目前规定要求在进行跨境信息传播之前，需要明确取得个人的同意，这给有国际运营和沟通的中国企业和外国企业带来了巨大的监管负担。 数据主体应该默认当他们进入电子商务市场，订阅金融服务或是参与一般性在线活动时，自己的信息就可能被利用。正式认可“默认同意”的标准将避免对现有数据采取重复性保护措施，并确保行业活动完全符合中国的政策。

- 中国决策者应与国际行业主体进行磋商，根据中国在保持监管透明度方面做出的国际承诺，结合全球最佳实践，制定并实施透明的数据安全管理政策。中国与他国政府的双边以及多边网络对话应该不局限于网络犯罪范畴，应与行业利益相关者围绕由于新出现的网络威胁和不断变化的监管问题所带来的运营挑战展开讨论。此外，中国还应就执法信息的交流机制进行双边和多边的讨论，确保国际司法问题的解决。

- 中国应成为《亚太经合组织跨境隐私保护规则体系》（CBPRS）的一员。该体系旨在建立消费者、企业和监管者对跨境个人信息流动的信任。我委员会还建议将遵循《亚太经合组织跨境隐私保护规则体系》作为将数据输出中国的合规基础。

- 中国应明确公布关于数据输出安全审查结果的申诉制度。中国还应明确指出网信办的权责，是仅限于协调指导，还是有权否决相关行业主管部门做出的决定。我委员会建议中央网信办明确表述行业主管部门和网信办的等级关系和职责划分，以及网信办将如何处理申诉。中国应限制强制性数据输出安全审查的频率，以缓解行业利益相关者承担的扰乱正常运营的行政负担。我委员会建议每三年进行一次强制性审查，以减轻行业利益相关者和监管机构的行政负担。相关规定要求，由行业利益相关者证明某个国家或地区足够安全，能够保护传输的数据。中国政府应取消该项规定，因为这远远超出了相关行业主体的能力范围，应由政府管理。

挑战二：市场准入与全球解决方案

由于中国的许可制度过于严苛，许多创新性云计算解决方案无法在中国使用。这些政策使外国企业和本土企业的在华运营成本、运营效率和信息安全等问题变得更加复杂。

例如，中华人民共和国工业和信息化部发布了《电信业务分类目录（2015 年版）》，为开展基础电信业务和增值电信业务的外国和中国企业做出了许可性规定。虽然该分类目录未使用 “云计算”这一术语，但它却涵盖了云计算的某些部分，并将其作为增值电信业务的一部分，这一分类方法在其他市场中并未被使用。因此，要在中国提供云解决方案，企业就必须获得三个不同的许可证——互联网数据中心许可证、互联网服务提供商许可证以及互联网内容提供商许可证（有时需要提供）。而外国企业还需要与中国当地企业建立合作关系才能获得这些许可证。虽然外国企业可能控制最多高达 50％的此类业务，但是有些跨国公司却无法申请或获得这些许可证。因此，许多国外的云服务在中国无法使用，这迫使在中国境外使用这些云服务的中国企业和外国企业在中国运营时不得不使用不同的系统。

对于购买全球云产品和云服务的企业来说，无论他们在何处开展业务，都应能够使用其购买的云产品和云服务——这正是云解决方案的核心目的和优势之一。无法完全使用购买的云产品和云服务阻碍了中国境内的团队与国际团队之间的有效沟通，进而影响了基于云的客户关系管理软件的使用，内部团队与外部客户之间共享商业文件，以及用于托管数据和为研发提供开发平台的云技术的应用。

虽然有许多中国本地的云解决方案可供使用，但是这些解决方案很少能够覆盖全球，这给在全球范围内使用中国云技术制造了障碍。这与中国的相关政策给在中国使用全球云产品制造的障碍类似。因此，中国的相关政策虽然可能会在中国国内市场上催生出重量级的角色，但却无法造就全球技术领导者——而与全球行业领先者在国内市场的竞争或将改善上述情况。

最后，这些限制性规定与“互联网+”和“十三五”规划等计划制定的目标背道而驰。这些计划旨在利用云计算来提升中国经济，如今却让其他市场从全球信息技术网络的高效率和安全性中受益。

几点建议

- 中国应同时允许中国企业和外国企业提供云计算服务。具体而言，我委员会建议工信部重新评估中国对云计算的监管方式，采用国际方法，将云计算总体归类为计算机服务而不是增值电信服务。这一改变将使中国的做法与国际最佳实践保持一致。

- 只要云计算服务在《电信业务分类目录（2015 年版）》中被定义为增值电信业务，中国的监管机构就应向在中国寻求提供云计算服务的外商独资企业和中外合资企业颁发互联网内容提供商许可证和互联网数据中心许可证。 我委员会还建议允许合资企业中的外国投资者保留对合资企业或其合作伙伴许可运营的软件和其他专有技术的所有权和控制权，以保障知识产权的合理保护并激励在中国使用最先进的技术。

- 中国应加强互联网数据中心许可证、互联网服务提供商许可证以及互联网内容提供商许可证的许可审批程序过程中的透明度，以便外国企业可以积极地与主管部门合作，解决涉及风险和安全要求的问题。

- 中国应允许行业利益相关者使用合法注册的虚拟专用网络（VPN）服务，以便他们出于合法的商业目的自由地访问全球互联网。在虚拟专用网络注册的过程中，中国应只规定统计虚拟专用网络的用户数量，而不要求提供用户的具体个人信息。

- 随着产品转为通过互联网向客户直接提供信息的解决方案，例如汽车上的车载显示系统，中国应明确定义符合互联网内容提供商许可要求的服务类型。

挑战三：安全可控的技术与过于宽泛的网络安全审查制度

企业使用全球技术系统以确保为客户的数据提供最高级别的安全保护，其中包括个人身份信息，防止数据被误用或盗用。为此，强制性要求采取或使用特有的“安全可控”技术的政策实际上可能不利于实现安全。

我委员会会员公司称，信息技术产品的本地采购招标仍然要求使用“安全可控”的技术，在实施过程中仅依据国别而非技术评估，就优先考虑中国本土产品而不是国外技术。

网信办已明确表示中国本土和外国的技术都有资格成为“安全可控”的技术，我委员会及会员公司对此表示赞赏。我们希望在对产品和服务进行安全审查的过程中，这些原则能够被严格地执行。

过去几年来，中国已经实施了对信息和通信技术产品的网络安全审查制度，却并未公布关于测试指南、产品范围、所需文件、时间表或其他许可程序等必要的细节信息。因此，目前尚不清楚这些制度将如何与现有的审查评估制度相互作用，如网络安全等级保护制度，其他非公开审查机制和《中国网络安全法》中概述的网络安全审查机制。

此外，一些草案和已颁布的法规要求使用本地加密算法，这一做法与全球最佳实践并不一致，会产生一定的安全隐患。跨国公司采用的是国际加密标准，国际专家已对其安全漏洞进行了广泛的测试，以最大限度地减少问题，确保客户的数据得到很好的保护，金融行业的法规对此有特别的要求。中国网络与全球网络采用不同的加密标准，可能彼此无法兼容，这可能会使中国境内的网络出现安全漏洞。这些风险与中国加强信息技术安全的总体目标背道而驰，也阻碍了中国企业进军全球最大市场，成为国际化企业的脚步。

最后，使用中国特有的技术系统将限制企业在中国境内应用能使中国消费者受益的全球解决方案和最佳实践。此外，强制性地要求采购本土产品可能意味着企业在中国使用的设备与其在全球业务中使用的设备无法兼容，抑或无法达到其在全球业务中使用设备的安全标准。将信息技术外包给全球服务商还是本地服务商，应取决于企业风险评估需求而不是政府指令，后者可能会阻碍企业优化其安全性能。

几点建议

- 网信办应确保在实施“安全可控”的技术这项要求时一视同仁，不会要求或优先考虑采购或使用中国本土的产品、技术、知识产权和标准。如果要求某种网络产品或服务进行“安全可控”的界定，那么界定范围应该根据产品和服务做出细致的调整。如果这些产品和服务无法满足安全要求，将会给国家安全带来具体的、实质性的风险。对于未被指定为关键信息基础设施运营商的技术用户，应完全免除其在采购安全可控的技术方面的要求。

- 中国应将其网络安全审查机制精简为单一的、明确的制度，为其审查范围内的产品类型设定狭义的参数，并提供关于许可要求、时间表、测试程序等其他信息的具体细节，

以方便公司遵守相关规定。该制度应该是透明的，在制定时应与国际行业主体进行磋商，以确保中国从其他市场中已实行的安全审查机制的经验中受益。任何网络安全审查制度也应明确表述其与现有的安全审查机制如网络安全等级保护制度之间的关系。这将提高效率，降低业务成本，并减少国际上对此类审查程序中可能出现的歧视产生的担忧。

- 中国应该在有第三方专家参与的网络安全审查流程中防止潜在的利益冲突，继续强化商业秘密保护机制。网信办还应制定相关的规定，禁止有明确利益冲突的专家进入申请人的审查专家小组，并要求专家组内存在利益冲突的人员退出审查。中国还应建立正式的申诉制度，以便出现利益冲突时，申请人能够向专家组提名人员提出自己的异议。该制度应制定一个公开的时间表，用以考虑、审查和解决争议，尽量减少投资过程中出现的干扰因素。为此，我委员会还建议允许需要进行网络安全审查的企业就专家组提名提出自己的意见。网信办应向企业提供最新的、完整的获批专家的名单，并允许他们向专家组提名一定数量的专家。最后，网信办应要求专家在解答信息请求时附上实际事实、商业经验和可靠的科学依据。

- 考虑到全球网络集成、基于风险的网络安全框架以及基于行业共同做法的全球安全标准，中国应允许企业使用单一的全球技术平台，采购最合适的，最能满足其企业安全需求的信息技术解决方案和产品。

- 中国应在今后起草技术安全标准的过程中与外国企业和行业协会磋商，以确保利用全球最佳实践，将中国和全球信息技术安全体系整合起来。技术安全标准草案不应包括披露源代码、使用本地加密标准、实行安全可控的或本地创新产品等强制性要求，否则可能会加重企业的负担，危害知识产权的使用和保护。

- 中国应确保技术安全标准草案与其在 2015 年商业联合会和 2016 年美中战略与经济对话中做出的承诺相一致，保证产品的技术安全不由其国别决定，而应通过对其安全性能和流程进行技术评估来确定。

- 国务院应要求所有新技术标准的征求意见期限为至少 60 天，并且不强制要求优先考虑中国国内的产品和服务。