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

优化互联：关于中国信息技术环境的思考与若干建议

2016年11月

信息技术（IT）创造了经济增长的新途径，彻底改变了公司的经营方式。作为世界上互联网用户数量最大的国家，中国已经成为全球创新中心。内容涉及移动应用开发、智能设备、电子商务、移动支付领域，还包括其他将大数据与互联网功能整合以提升传统商业模式的技术前沿。

与此同时，全球各国政府面临的挑战是，如何管理新技术的发展，从而使得所有用户都能高效、安全地使用，同时又能兼顾政府的合理要求与企业和个人的需求。和世界上其他各国一样，中国的政策制定者正在制定保护数据隐私和信息安全方面的措施，因为新技术的发展对传统的监管框架提出了挑战，并要求其做出改变。

美中贸易全国委员会（USCBC）2016年的会员报告显示，79%的会员公司对中国管理信息流动和技术安全的方式表示关切，主要是因为相关政策对公司开展日常业务的能力产生了影响。目前中国的监管制度对国内外公司运营产生的影响，不同于世界其他国家。中国的许多政策尚未明确表述有关创新和技术安全方面的全球最佳实践是否可以在中国应用。因此，许多技术解决方案在中国被限制使用，而这些解决方案已有全球验证的技术保障，能够有效提高运行效率，包括打击安全威胁的信息交流。而这些政策正在影响全球数字经济的发展。

基于对会员公司技术高管的大量访谈，美中贸易全国委员会的建议涉及公司在中国使用信息技术时面临的一些具体障碍，同时也提供了能够协调公司运营和安全需求的潜在解决方案。这些建议旨在提出建设性方案，以务实的方式解决各方关切的问题。美中贸易全国委员会感谢有机会提出这些建议，并希望与中国的监管机构就此展开讨论。

挑战一： 数据流动与数据本地化

中国的数据政策使在华公司与其全球其他分支机构之间的沟通不畅，阻碍了跨境创新，并因要求安装重复性的信息技术基础设施增加了其经营成本。这些政策导致公司无法正常使用其全球专业知识和技术，这也制约中国依托互联网+、大数据战略等创新计划的发展。这些限制影响了外国在华企业和国内公司经营全球平台，开展电子商务和进行最前沿研发的能力。

以下两种类型的数据政策影响了公司运营：

- 数据本地化政策要求公司在中国存储特定类型的数据。这些政策要求公司使用独立于其在全球其他地区运营活动中使用的设施之外的本地基础设施进行数据托管和处理。
- 数据流动政策限制了信息的跨境流动。数据流动是现代化、国际化、以及数字化经济的关键组成部分，让中外公司最大限度地在其运营的国家提高效率和确保金融交易的完整性。中国在金融服务，医疗和其他行业的法规中禁止特定数据在中国的跨境流动。此外，中国目前的法规尚未明确哪些类型的数据可能会被视为“国家机密”，从而增加了公司在无意识的情况下因转移信息而违反法律的风险。

为撰写关于信息通信技术（ICT）在华最佳实践的相关报告，美中贸易全国委员会开展了大量访谈。访谈中，会员公司技术高管表示，中国的数据流动和本地化政策使得他们难以在中国使用大数据开展产品支持、产品安全和产品创新方面的分析。例如，外资能源公司在中国运营的风力发电机组产生的数据需要与其全球总部随时保持沟通，以便其全球团队可以响应停电事件并预防事故。为智能设备提供高科技、互联网连接的公司需要访问这些设备上的数据，以便进行远程维护和维修。从事国际电子商务的公司依靠信息流动，通过跟踪跨境可疑活动来防止跨境身份盗用犯罪。金融服务公司通过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，以及识别潜在的非法交易活动。过度限制性的数据政策阻碍了上述类别的活动，限制了公司使用全球最佳实践的潜力。

虽然这些政策指定的出发点旨在保护公民的个人信息安全，但是要求数据本地化和禁止数据跨境流动对实现该目标收效甚微。保护数据隐私最严格的国际标准应由行业共识确定，借鉴全球最佳实践，并且在很大程度上不涉及数据存储或传输的位置。网络安全专家也认同，信息的安全性取决于使用的技术类型、用户的专业知识和良好的制度实践，而不是数据所在的地理位置。

确保数据跨境自由流动是创新型数字经济的重要组成部分，中国已将其作为优先发展事项。中国的“十三五规划”，“中国制造2025”和“互联网+”等规划也都强调了基于智能和互联网技术的发展。政府高级官员在讲话中经常强调在中国境内和20国集团框架下互联网开放和互联互通的重要性。这些努力可以通过采用跨国公司提供的最佳实践和专业知识得到加强，因为跨国公司具有整合传统商业实践与全球信息网络的经验。允许公司、其支持团队和互动产品在全球范围内访问这些信息，是“十三五规划”的目标中“智能技术”的一个关键组成部分，同时也是成功制定跨行业高层政策所必需，例如“互联网+”、“大数据推广计划”，以及通过智慧城市和中国金融业实现更高能效的发展计划。

几点建议

- 在颁布过度严苛的法规之前，中国应详细分析在创新性和全球性数字经济中限制数据有效流动的相关成本，同时考虑到国内产业、全球商业、研发以及网络威胁管理的相关成本。中国的安全审查制度和数据安全许可制度应基于这些详细的分析来确定是否有必要设置，中国应淘汰那些制约全球数字经济增长的不必要的安全审查制度和数据安全许可制度以允许数据跨境流动。中国的监管机构应确保数据流动政策

与国际公认的网络安全最佳实践保持一致，包括修改《网络安全法》中对信息有效流动不必要的限制规定。

- 中国应就归类为“国家机密”的数据类型提供更详细的定义，以确保公司不会在无意中违反关于此类信息存储和传输的法律法规；应进一步界定其适用范围，使其只包括关乎国家安全的重大信息。
- 中国应允许将数据副本发送到国外进行分析和处理，以确保公司的运营效率并鼓励使用大数据进行创新。这不仅保障了数据的区域管辖权，同时允许公司能够开展重要的业务活动。
- 中国的决策者应与国际行业就数据安全管理的全球最佳实践进行磋商。这些政策应以明确、透明的方式，遵循中国在透明监管方面的国际义务来制定。
- 中国应定期与其他政府就网络相关问题进行对话，确保其政策采用全球最佳实践、最前沿的认识和解决方案，进而确保制定出最佳的监管制度。此外，中国应就执法案件相关的信息交流机制进行双边和多边讨论，确保解决国际管辖权问题。
- 中国应发展开放且稳定可靠的互联网，以便公司获得进行创新和国际商务所需的信息流动。中国的监管机构应与运营互联网相关业务的公司合作，开发解决方案，从而使他们能够为中国用户提供服务。
- 中国应成为《亚太经合组织跨境隐私规则体系》（CBPRS）的参与国，该体系旨在在个人信息跨境流动中建立消费者、商业公司和监管机构之间的信任。在《亚太经合组织跨境隐私规则体系》的框架下，独立的第三方问责机构将确保国家和公司的数据保护机制与该框架的要求相一致，并符合合理且可执行的保护公民隐私的标准。

挑战二： 市场准入与全球解决方案

由于中国的许可制度不够明确，许多创新性云计算解决方案在中国无法使用。这些政策使中国境内的中外公司的业务成本、效率和信息安全问题更加复杂化。

例如，工业和信息化部（MIIT）发布的《2015年电信业务分类目录》（以下称“《目录》”）规定了外国公司和中国公司开展基本电信服务（BTS）和增值电信服务（VATS）的许可要求。虽然《目录》中没有使用“云计算”这一术语，但它确实将“云计算”的要素涵盖为增值电信服务的一部分，而这一做法在其他国家尚未出现。因此，为了在中国提供云服务解决方案，公司必须取得三个不同的认证许可——互联网数据中心（IDC）许可证、互联网服务提供商（ISP）许可证，以及有时还需要的互联网内容提供商（ICP）许可证。外国公司必须与本土企业建立合作伙伴关系才能取得这些许可证。虽然外国公司可以控制最高达50%的运营，但是一些跨国公司在实际申请和取得许可证时遇到困难。因此，许多外国云服务在中国并不可用，迫使中外企业在中国的运营活动中使用不同于其境外的技术支持和维护系统。

购买全球云产品的公司有理由期望无论他们在何处运营，都能使用其购买的云产品——这是云计算解决方案的核心目的之一。上述规定影响到中国境内团队与国际团队之间的高效沟通，进而影响到基于云的客户关系管理（CRM）软件的使用，不利于内部团队之

间、内部团队与外部客户之间共享业务文档，也不利于云技术在托管数据和提供研发平台方面的应用。

虽然有多个中国本地云解决方案可用，但仅有为数不多的解决方案具有全球通用性，这本身也是阻碍了中国云技术在全球的广泛应用。这与现行政策下中国无法使用全球云产品的道理是一样的。因此，中国的政策可能使其国内市场出现力量雄厚的技术参与者，却不能造就全球技术领导者——如果国内能形成与全球行业领先者的竞争，这一情况将可以得到改善。

无法链接全球和中国境内的网络也会产生安全风险。本地软件或本地供应商可能无法解决或沟通使用全球技术时出现的问题。当出现维护问题、技术问题或网络犯罪渗透时，断裂的全球通信网络会限制公司快速响应的能力。

最后，这些限制性规定意味着，旨在利用云计算提升中国经济的政策目标将不能实现，如“互联网+”和“十三五规划”等，因为这些限制性规定不但无益于中国市场，反而令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

- 中国应重新考虑工业和信息化部《电信业务分类目录》中被归为云计算服务的许可要求，确保国内外公司能够提供这些服务，使得其规定与其他国际市场处理类似服务的规定相一致。
- 只要云计算服务被归为2015年工业和信息化部《电信业务分类目录》下的增值服务，中国的监管机构就应向希望在中国提供云计算服务的外商独资企业（WFOEs）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。
- 中国应提高互联网数据中心(IDC)、互联网服务提供商(ISP)和互联网内容提供商(ICP)许可审批流程的透明度，以便外国公司能够积极与监管机构合作，解决风险和安全要求方面的问题。
- 随着产品趋向于更加互联的呈现方式，即通过互联网直接向客户提供信息，如车辆上安装的车载显示系统，中国应明确界定符合互联网内容提供商要求的服务类型。

挑战三: 安全可控的技术与过度宽泛的网络安全审查制度

为保护客户数据免受犯罪分子攻击，跨国公司通常会利用全球技术系统以确保为客户提供最高级别的安全保障。因此，要求公司接受或使用独特的“安全可控”技术，实际上可能对实现其安全目标产生相反的作用。该术语的确切定义尚未明晰，但似乎是基于一个并不准确的假设，即国内产品比国外产品更安全。

会员公司注意到，针对信息技术产品的本地采购招标仍然呼吁使用“安全可控”的技术，并且在招标过程中仅依据国籍，而非技术评估，就优先考虑本地产品。“安全可控”在政府部门指定的金融服务领域的技术政策草案中也不断被提及，有些法规草案规定到2019 年国内技术的使用率应达到 75%。此外，一些推进“安全可控”技术的法规草案包

含了公开源代码的要求。而源代码是知识产权（IP）项目，通常不对技术使用者开放并且根据法律禁止向第三方提供。

在过去几年中，中国没有提供关于测试指南、产品范围、所需文件、时间表或其他许可程序的必要信息。而在此情况下，中国实施了针对信息通信产品的网络安全审查制度。因此，目前还不清楚这些制度如何与现有的审查评估相兼容，如信息安全等级保护制度（MLPS）、其他非公共审查机制、或《网络安全法》草案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，这种做法与全球最佳实践并不一致，并且引发了安全关切。跨国公司使用的是国际加密标准，其安全漏洞已经由国际专家高强度测试，以便最大限度地减少问题，确保客户数据得到良好的保护——这正是金融行业法规特别要求的。中国网络采用与全球网络不同的、而且可能是互不兼容的加密标准，这可能导致在中国特定网络中产生安全隐患。这些风险不利于中国实现加强信息技术安全的总体目标。

最后，使用中国独有的技术系统将限制公司在中国境内应用全球解决方案和最佳实践，不利于中国消费者从中受益。此外，从本地合作伙伴处进行采购可能意味着使用的设备不兼容或低于公司为其全球运营设定的安全标准。信息技术合同选择与全球还是本地合作伙伴签订，应由公司风险评估需求决定而不是由政府指令规定。

几点建议

- 中共中央网络安全和信息化领导小组办公室（CAC）应确保其在全国信息安全标准化技术委员会（TC260）中制定的“安全可控技术”的定义是非歧视性的，定义制定过程透明，且不强制或优先采购使用源自中国的产品、技术、知识产权和标准。
- 中国应将其网络安全审查机制简化为单一、明晰的制度，为审查范围内的产品类型设定明确可依的参数，并提供有关许可要求、时间表、检测程序和其他信息的详细要求，以便公司有规可循。这一制度应该是透明的，应与国际行业协商制定，从而确保中国将从现有的已被其他市场利用的安全审查机制中受益。任何网络安全审查制度还应明确其与现有安全机制的适用关系，如《网络安全等级保护制度》。这将确保审查流程更有效，降低公司业务成本，同时减少国际社会对这些制度中潜在歧视问题的关注。
- 中国应允许公司使用统一的全球技术平台，并在全球网络集成、基于风险的网络安全框架，和基于行业通用的全球安全标准等的基础上，采购最适合企业和安全需求的信息技术解决方案和产品。
- 中国应与外国公司和行业协会协商起草技术安全标准，包括安全可控技术的安全标准，确保引入全球最佳实践，从而进一步整合中国和全球信息技术安全制度。关于技术安全标准的草案不应包含公开源代码、使用本地加密标准，或其他危及知识产权的使用和保护的要求。
- 有关技术安全标准的草案应反映中国在2015年联合商贸委员会和2016年战略经济对话中做出的承诺，即技术安全本身不应与产品国籍有关，而应通过对其安全功能和过程的技术评估来确定。