
ISC
2015
中国互联网安全大会
360互联网安全中心
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
网络空间安全战略论坛

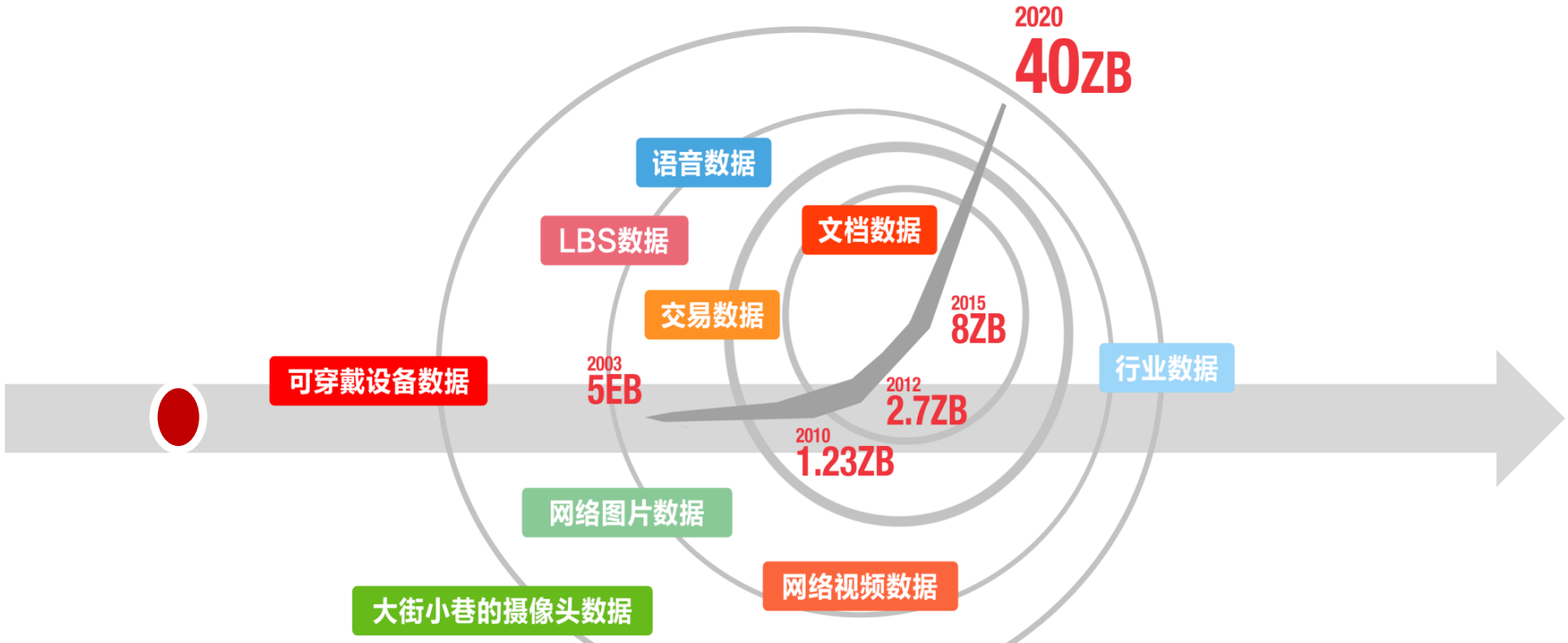
# 网络空间安全体系中的跨境数据流构建

吕本富

中国科学院大学教授、 国家创新与发展研究会副理事长

# 前 言

# 数据体量的跃升：从TB到PB




1024GB=1TB；1024TB=1PB；
1024PB=1EB；1024 EB=1ZB；
1024ZB=1YB。

数据体量从TB级别跃升到PB级别。

# “数据—原油”

在数据世界中，大量利润是通过使用人工生成的信息得到的。人们的浏览习惯、聊天记录、移动轨迹以及地点定位——所有这些东西都被商业化了。这些都是极为私人化的数据，尽管通常情况下人们并不这样认为。

可以将私人数据与化石燃料进行一种行之有效的比较：原油是从死去很久的微生物身体中压缩得来的，而私人数据则是通过对人们私人生活碎片的压榨而产生的。这些数据实际是人类经验的一个浓缩。

# 帕兰提尔公司

一家名叫帕兰提尔（Palantir）的初创公司帮助美军捕杀了奥萨马·本·拉登（Osama bin Laden）。帕兰提尔公司的客户包括美国国家安全局（NSA）、美国联邦调查局（FBI）、美国中央情报局（CIA，通过其In-Q-Tel风险投资基金成为该公司的早期投资人）和很多其他的美国反恐和军事机构。

在过去五年里，帕兰提尔公司已经变成了进行大规模数据挖掘以供美国情报及执法部门使用的关键公司，其软件产品有着流畅的界面，旗下程序员甚至会空降到客户的总部进行程序定制。

帕兰提尔公司把混乱无序的大量信息变成直观的可视化地理分布图、柱状图和关联图。只要给该公司所谓的“前沿部署工程师们”几天时间，让他们分析、标记和整合所有零碎的客户数据，帕兰提尔公司就能弄清楚各种各样的问题，例如恐怖主义、灾难响应和人口贩卖。

# 一、跨境数据流成为焦点

# 新技术带来整体网络环境的变化

- **跨境数据流动的现象早已经存在，如国际间的航空、贸易以及金融等领域，都牵涉跨境数据流动。我们现在进行的是随着云服务和大数据新技术的发展带来的跨境数据流动的规模化和复杂性研究。**

1978年由78个国家代表团参加的政府间信息局国际会议就曾发表报告，认为跨境数据流动“将国家置于危险境地”。受制于当时的客观条件，各界对跨境数据流动的认识不及大数据和云计算时代那么全面，但是可以体现出跨境数据流动问题的广泛性和深远性。

# 数据跨境流动出现了急剧增长

**如果政策制定者可以设计共享规则鼓励信息的自由流动,更多的人会有更大的信息获取和信息将被创建并交换**

2005年到2012年之间跨境互联网流量增长了18倍。

从2000 到2012年全球在线流量增加了500倍

知识密集型信息流是劳动密集型的增长速度的1.3倍。

数字化的商品(如音乐和电影)变化的混合流动,改变全球物流和启用新的和较小的玩家参与贸易

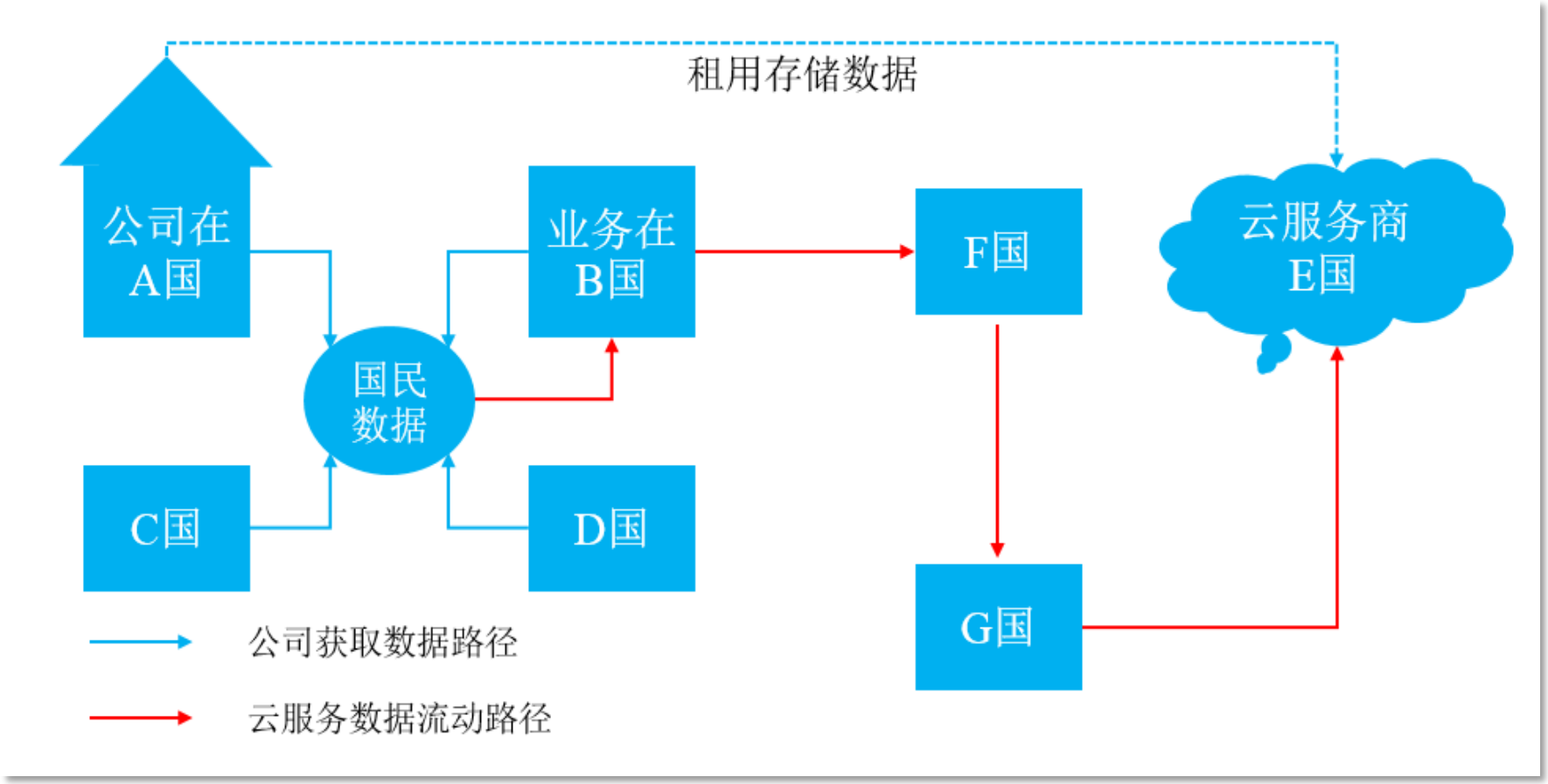
麦肯锡全球研究院:2014、2 - 3和eBay 2014

# 数据所有者面临的安全挑战

- 文档被数字化并进一步网络化，所有者原有的基于位置和物理的控制力在减弱。
- 数据所在地管辖权所有人更容易访问数据。
- 当出现纠纷时，数据所有者缺乏法律支持和举证能力。

# 二、多利益相关方构成的数据流架构

# 一个跨境数据流动架构示例



# 什么数据在流动？

| 要求<br>部门/案例 | 数据保护 | 知识产权 | 保密协议 | 过时的传统法 | 信息安全相关 | 监管审查 | 国家主权 | 国家安全 | 司法管辖权/可执行性 | 采购条例 |
|---|---|---|---|---|---|---|---|---|---|---|
| 一般公共部门 | √ | | √ | √ | √ | √ | √ | √ | √ | √ |
| 征税和社会安全 | √ | | √ | | √ | √ | √ | √ | √ | |
| 医疗卫生和法律服务 | √ | | √ | | √ | √ | | √ | √ | |
| 媒体和娱乐 | √ | √ | √ | √ | √ | √ | | | √ | |
| 金融服务 | √ | | √ | √ | √ | √ | | √ | √ | |
| 国家档案 | √ | | | | | | √ | | √ | |
| 制造业/消费者 | | √ | | | √ | | | | | |

已知的跨部门要求概况，“√”表示优先考虑

来源：The European Cloud Partnership Steering Board

# 跨境数据流动问题牵涉多议题

全球贸易规则

知识产权

国家安全

互联网开放

# 利益相关方：国家、企业、个人

- **国家**

国家对其政权管辖地域范围内个人、企业和相关组织所产生的数据拥有的最高权力

- **企业**

互联网企业、IT企业对于用户在本公司产品上产生的数据，在用户许可的情况下，拥有对数据的部分使用权、开发权

- **个人**

用户对个人的数据拥有所有权

# 利益相关方冲突在哪里：国家与国家

- 数据控制弱势国家的敏感性
- 双边数据流动与保护力度不对等
- WTO多边框架下的贸易自由流通与各国不同安全诉求的冲突

# 利益相关方冲突在哪里：国家与企业

- 企业认为跨境数据制度建立带来的监管和市场准入障碍会影响云计算对经济的促进作用
- 不希望将国家安全与企业数据跨境流动混为一谈
- 繁琐的跨境数据流动制度会增加企业的成本和风险，在全球化竞争中将处于不利的地位

# 利益相关方冲突在哪里：诉求原则不同

- **主权国家**

要解决跨境数据流动带来的主权与治权的分离问题，考虑国家安全问题

- **企业**

希望信息自由流动，或者形成全球一直的的技术标准、制度框架原则

- **个人**

应用体验好；同时关注隐私保护

# 三、各国数据制度和法律

# 美国

**美国表面宽泛自由的数据政策背后是一套严谨的审查逻辑体系，对事关国家安全的数据存储和流动有着极为严格的要求。**

- 在美国，关于数据管理条例 — — 包括 HIPAA、HITECH、GLBA、SOX和 FISMA — — 并不具体管理存储数据的物理位置
- 组织法规中对安全性的标准可能会限制位置移动。
- 出于法律差异性带来的风险考虑，组织通常会将远程存储的敏感信息或知识产权保留在美国本土。

# 欧盟

**欧盟数据保护的监管出发点是严格控制本人数据流动，信息处理原则上应获得数据主体同意。**

- 对内，欧盟通过指令为成员国确定了数据保护的标准，禁止成员国借数据保护的名义限制个人信息在欧盟境内的自由流动。
- 对外，以数据接受国是否达到数据保护的充分性要求，向欧盟境外转移数据将受到限制。
- 由于美国未被欧盟认定充分保护的资格，为了实现欧盟向美国的跨境数据转移，经过多次磋商，2000年 3 月美国与欧盟达成了安全港协议。

# 俄罗斯

**《个人数据保护法》对公民个人数据保护作出了规定，要求俄罗斯公民的个人信息数据只能存于俄境内的服务器中，以实现数据本地化。**

- 法律对签证办理、机票购买、媒体行为和法院行为等进行了例外规定。
- 另外，据媒体报道美国苹果公司和eBay公司已经表示遵循俄罗斯的新政，在俄罗斯本地存储用户数据。

# 跨境数据流动问题上各国尚未完全找到共同点

**可见，各国的决策者还没有完全在国际条约或协定设计上找到共同点，来明确如何协调数据的跨境流动**

| 各国/各地的政策权重不同 | 各国/各地的部门职能分工不同 |
| --- | --- |
| 以欧盟和美国为例：欧盟对于数字版权要求更高，高度监管着互联网服务提供商要符合数据保护规则，而对于言论自由的保护程度低于美国。 | 在美国,各州可以制定商业规则制度,而在华盛顿立法和行政部门制定贸易、人权、国家安全政策。相比之下，欧盟，如国家安全政策的一些政策制定上仅仅在国家层面上，而数据保护和人权等政策制定存在于国家和欧盟层面，而贸易政策在欧盟层面。 |

# 四、解决机制：多边对话

# 各利益相关方冲突——解决机制不同

- **主权国家**
  - 根据自身的安全诉求，限定跨境数据流动政策限制，实施跨境许可管控
  - 进行双边数据流动保护谈判
- **企业**
  - 倡导以领先的云服务商来在实践中积累技术标准、法律标准和运营保障的解决方案。政府、公民、云服务和云用户摸索共识，来促成这些障碍的解决
  - 推动数据自由流动被纳入到全球贸易规则中
- **地区性、政府间、综合性的国际组织**
  - 以欧盟为例-数据保护充分性审核机制；以欧盟为主体签订双边数据保护协议

# 具有网络治理职能的多边组织

| 名称 | 类别 | 取向 |
| --- | --- | --- |
| **事件响应和安全团队论坛（FIRST）** | 主权国家背景的跨国技术工作论坛 | 能力建设，问题解决与制度建设 |
| **八国集团（G8）** | 多边政府间国际组织 | 能力建设，制度建设与跨国协调合作 |
| **电机及电子学工程师联合会（IEEE）** | 专业技术人员构成的国际组织组织 | 技术标准建设 |
| **互联网治理论坛（IGF）** | 跨国论坛 | 观念与信息交流 |
| **国际刑警组织（INTERPOL）** | 政府间合作组织 | 聚焦打击计算机、网络犯罪 |
| **Meridian进程** | 政府间合作机制 | 聚焦关键基础设施保障的政府间合作机制，并正试图将合作范围扩展到工业控制系统 |
| **北大西洋公约组织（NATO）** | 军事同盟、政治同盟 | 聚焦美国及其核心军事盟友的网络安全，网络战 |
| **欧洲联盟（EU）** | 区域性国际组织，主权国家构成的一体化组织 | 能力建设，制度与跨国合作，强调全面的网络安全能力 |
| **国际电信联盟（ITU）** | 联合国下属的政府间国际组织 | 能力建设，国际发展与跨国协调 |
| **美洲国家组织（OAS）** | 政治同盟 | 聚焦反恐、网络安全标准以及打击网络犯罪 |
| **经济合作与发展组织（OECD）** | 基于意识形态的政府间国际组织，政治联盟 | 内部成员的网络安全与隐私政策协调 |
| **欧洲理事会（EC）** | 区域性多边国际组织，政治联盟背景 | 制度与跨国合作，侧重打击网络犯罪方向 |
| **亚太经济合作组织（APEC）** | 区域性多边国际组织 | 制度与跨国合作 |
| **东南亚国际组织（ASEAN）** | 区域性多边国际组织，军事联盟背景 | 制度与跨国合作 |

# WTO：传统多边贸易组织协调范围延伸争论

- **支持者**
  - WTO作为国际多边贸易的重要组织，数据交易绕不开WTO；
  - WTO管辖范围包括所有货物贸易和服务，包括通过互联网的国际贸易。因此在此基础上对原有贸易类别进行适度扩展，能够使原有贸易原则适用于在线服务。

- **反对者**
  - 数据流动不仅仅是贸易问题，还涉及隐私和人权。WTO原有政策框在设计时“没有做好准备在隐私和人权问题上设计弹性的语言”。

# 五、解决方案

# 数据安全港：双边对话机制尝试

- **成果**
  - 2000年 3 月美国与欧盟达成了安全港协议。
  - 安全港协议的数据处理要求包括：通知、选择、连续转移、安全、数据一致性、获取、执行等。这些原则体现了信息主体的知情权、选择权、获取权、异议权、救济权等权力，给加入安全港的公司设置了公开透明、目的限定、特殊敏感信息处理、数据质量、安全措施、异议处理等责任和义务。
- **不完善之处**
  - 协议是双方让步的结果，但是这一协议下仍存在着很多安全风险，如法律本身的不确定性约束了安全港协议，导致很难审查数据进出口商是否遵循了协议。
  - 额外的问题包括：法律资格的不确定性,含糊的原则与常见问题解答,以及宽松的执行协议,导致协议的越来越不可信,不仅是协议本身,也在美国当局执行。

# 以战略高度解决数据自由流动和贸易问题

- 互联网是为了确保技术的互操作性,协作开发和透明度。
- 但孤立的政策使互操作性,跨边界合作,和透明度更难实现。
- 政策制定者必须更加战略性地考虑如何最好地促进跨境信息的自由流动和贸易协定。

# 感谢聆听！