CSA GCR cloud security alliance GREATER CHINA REGION ®

# 隐私科技行业总览

Nicolas 徐震天

电话/微信：13817139754

邮箱：xzt0621@aliyun.com

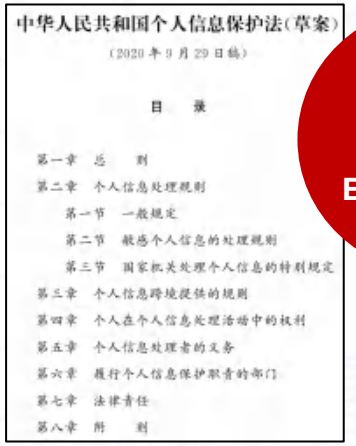
# 隐私科技的驱动力与市场玩家

## 隐私合规与保护

**世界各国和地区对于隐私保护均有着越来越严格的法律法规要求**






中华人民共和国个人信息保护法（草案）

（2020年10月21日稿）

目　录

第一章　总　则
第二章　个人信息处理规则
　第一节　一般规定
　第二节　敏感个人信息的处理规则
　第三节　国家机关处理个人信息的特别规定
第三章　个人信息跨境提供的规则
第四章　个人在个人信息处理活动中的权利
第五章　个人信息处理者的义务
第六章　履行个人信息保护职责的部门
第七章　法律责任
第八章　附　则

Ethic & Trust

## 数据价值最大化

**如何打通融合多方数据，创造整合多维数据、释放更大价值的机会?**

### 分散性

★数据持续不断的产生，来源非常分散，在数据生命周期的各个阶段如获取、存储、传输、验证及共享等阶段，缺乏明确的交互标准

### 复制成本低

★导致数据所有方不愿意分享数据，从而造成数据孤岛

### 价值聚合性

★单一数据源的价值有限，多维度数据或海量数据的价值明显更高

## Who are the Players

### 政府

- 一方面，制定各类法律法规与行业要求，通过“事前控制、事中监督、事后审计”的方式“守住底线”
- 另一方面，政府通过各类政策促进行业与技术的持续发展
- 最后，部分政府政务机构也是隐私科技的用户和受益者

### 用户（企业）

- 理论上所有行业、所有企业均会成为隐私科技的受益者
- 目前需求场景较多的行业包括金融、医疗、政务领域、教育、电商等等

### 厂商（平台）

- 互联网大厂：拥有丰富的数据生态和应用场景
- 创业公司：定制化服务、深耕某个细分赛道
- 咨询机构：独立性强且服务的深度与广度兼具
- 产业背景公司：行业聚焦性强
- 传统安全厂商：较为深厚的技术资源和客户资源

# How is the Market –产业图景

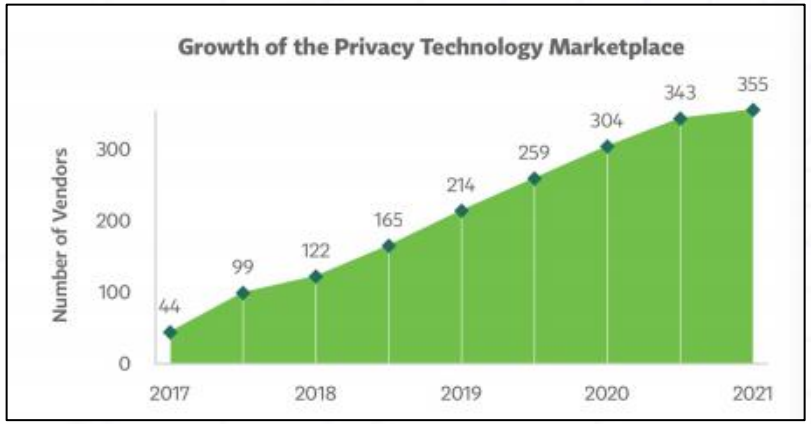
## 什么是隐私科技

-采用数字化的手段解决数字化时代下的隐私保护痛点。

-Privacy-enhancing technologies are technologies that embody fundamental data protection principles by minimizing personal data use, maximizing data security, and empowering individuals. -- *Gartner*

## 市场规模

- 从全球市场来看，隐私科技相关企业数量和市场规模自2018年GDPR正式生效以来，正经历着飞速发展的阶段。根据隐私保护行业权威组织IAPP的统计，2020年底隐私科技业务在全球范围内已达千亿市场规模。2021年，全球范围内有355家相关企业参与了IAPP全球隐私科技服务商调查，这一数字是2016年的9倍。代表性服务商包括One Trust, Big ID等。
- 从中国市场来看，根据行业数据显示，2024年隐私科技相关产业规模将有望触达100-200亿人民币的市场规模。代表性玩家如微众银行、腾讯、蚂蚁、字节、百度等。





*数据来源：2021 隐私计算行业研究报告，微众银行*

## Service Offering

**全球市场：**根据IAPP的统计模型，隐私科技可细分为11个不同的赛道：

| | | |
|---|---|---|
| Assessment Manager | Consent Manager | Data Mapping Tool |
| Data subject Request | Incident Response | Privacy Information Manager |
| Website Scanning | Activity Monitoring | Data Discovery |
| Deidentification/Pseudonymity | Enterprise Communication | |

**中国市场**目前还处于起步阶段，与全球市场相比，服务类型的颗粒度较粗，可大致分为三类：

1）提供资源生态和整体解决方案；

2）提供特定的底层技术及适用场景的解决方案；

3）深耕某一行业，提供行业特定的解决方案

| 公司 | 所属生态 | 核心产品 | 主要技术路线 | 开源与否 | 应用行业 |
|---|---|---|---|---|---|
| 微众银行 | 金融机构 | FATE，WeDPR | 联邦学习，区块链 | 是 | 金融为主 |
| 腾讯 | 互联网公司 | 腾讯安全联邦学习、神盾联邦学习平台，底层框架Angel PowerFL | 联邦学习 | 底层框架开源 | 金融，政务 |
| 蚂蚁 | 阿里生态，互联网公司 | 蚂蚁摩斯 | MPC+TEE，区块链 | 否 | 金融 |
| 百度 | 互联网公司 | 点石，MesaTEE，PaddleFL | 联邦学习，MPC+TEE | 逐步开源 | 政务，舆情 |
| 字节跳动 | 互联网公司 | Fedlearner | 联邦学习 | 是 | 电商、金融、教育 |
| 光之树 | 创业公司 | 天机可信计算框架，云间联邦学习平台 | 联邦学习，MPC+TEE | 否 | 金融为主 |
| 翼方健数 | 创业公司 | 翼数坊 | MPC等多种技术 | 否 | 医疗为主 |
| 富数科技 | 创业公司 | Avatar，FMPC安全计算产品 | 联邦学习，MPC | 否 | 金融，医疗 |
| 矩阵元 | 创业公司 | Rosetta，PlatONE | 区块链，MPC | 是 | 金融 |
| 同盾科技 | 金融垂直行业公司 | 智邦iBond平台 | MPC，联邦学习 | 否 | 金融 |

*数据来源：2021 隐私计算行业研究报告，微众银行*

# How is the Market –Service Offering和商业模式分析

## 全球市场

- 国外的隐私科技市场已进入了相对成熟的阶段，绝大多数服务都已产品化和工具化。
- 从Service Offering的角度来看，主要分为两类：一类以提供Visibility为主，向用户展示其收集&存储&使用个人信息的情况，代表性服务如Data Mapping Tool, Data Discovery Tool等；第二类为Take Action为主，目的是帮助企业更加安全/合规的处理个人隐私数据，代表性服务Deidentification, Website Scanning等。
- 从服务模式的角度来看，主要有产品模式和服务模式(SaaS)
- 代表性厂商包括OneTrust, Big ID等。

**产品销售模式—**服务商提供传统软件&产品的销售模式，费用按照系统消耗的资源、节点数量计算

**服务模式—**厂商提供SaaS平台，或根据客户需求的定制化服务。

**Assessment Manager**
通过自动化工具，实施隐私合规评估与风险评估。

**Consent Manager**
跨平台的获取、追踪、展示和管理“用户同意”

**Data Mapping Tool**
协助用户自动化的识别并获取Data Flow

**Data subject Request**
帮助用户更有效的更总和管理Data Subject提出的各类需求

**Incident Response**
隐私数据泄漏事件响应，包括通知、调查、mitigation等等

**Privacy Information Manager**
通过自动化平台时时更新、展示最新的隐私合规要求

**Website Scanning**
对网站或平台进行扫描，识别个人信息收集和传输的情况

**Deidentification/Pseudonymity**
隐私计算工具，对数据进行匿名化和去标识化

**Data Discovery**
通过工具，可视化组织内部个人信息的位置、类型，full visibility

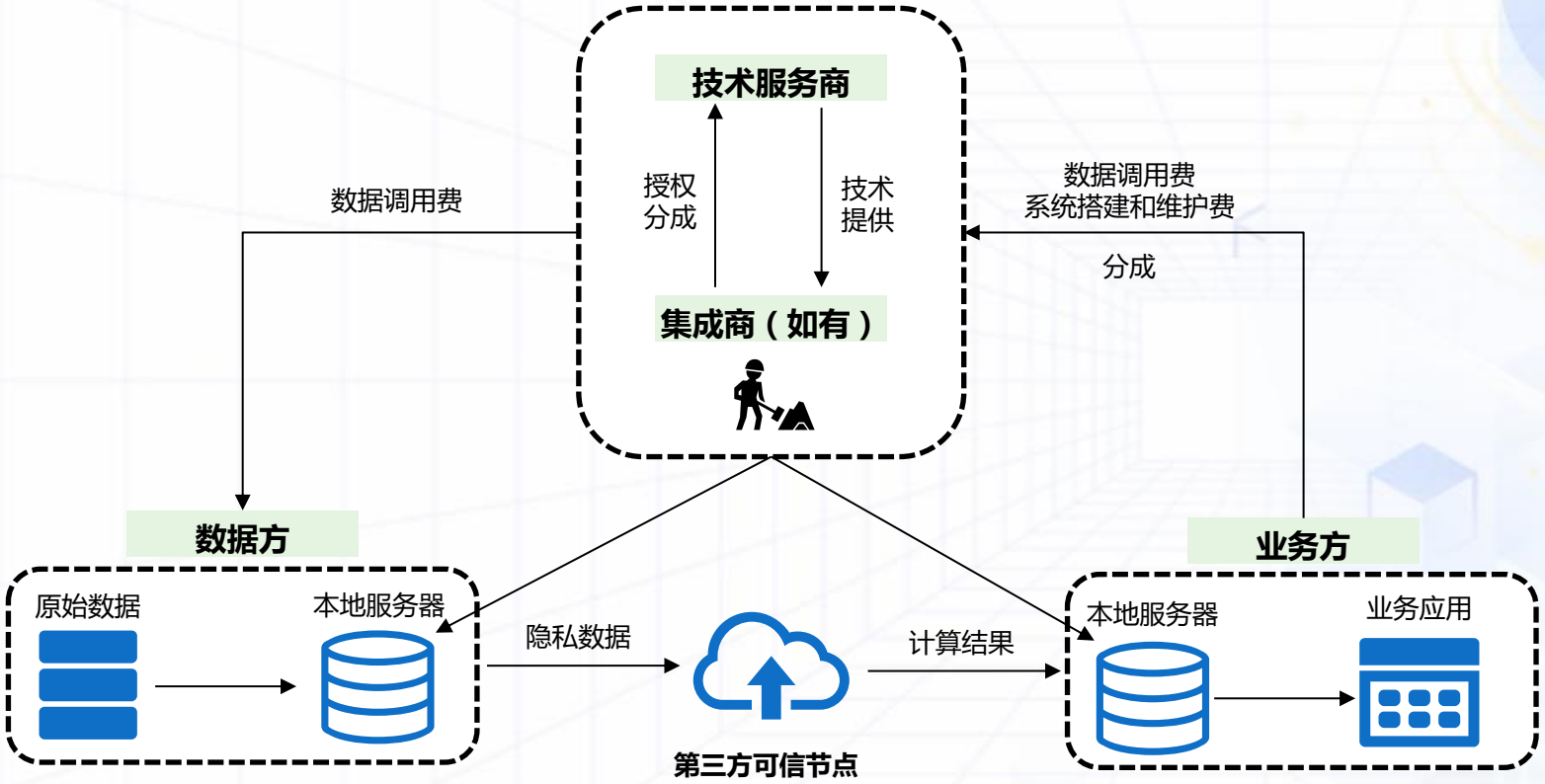
**Activity Monitoring**
监控平台/服务，识别企业内部对个人信息的处理活动

**Enterprise Communication**
加密平台/服务，用于企业内部通信如 Email等


# How is the Market –Service Offering和商业模式分析

## 中国市场

*相比于国外成熟的“隐私科技”行业，中国处于较为早期的阶段，服务内容主要集中于少数行业&企业的“隐私计算”产品与解决方案*




**产品销售模式—**服务商提供传统软件&产品的销售模式，费用按照系统消耗的资源、节点数量计算

**咨询与服务模式—**服务商为客户提供算法&模型调整、系统&产品运维等服务

**调用模式—**服务商为客户搭建系统，并作为收费通道代数据方向客户收取费用，收取手续费

**分润模式—**业务方早期并不需要系统搭建费，相当于技术服务商与客户联合运营业务。基于系统接入数据源，原有业务改善或新业务开展之后，双方根据业务实际效果分润

**业务方—**数据使用方（客户），如金融机构、政府机构、医疗机构、各行业企业等等；

**数据方—**数据源，如互联网大厂、征信公司、各地大数据局等；某些情况下数据方也是业务方

**服务商—**隐私科技服务商，为业务方提供解决方案或服务。特定场景下数据方也可以为服务商（如互联网大厂）

# 路在何方—痛点与未来发展方向的思考

## 法律与政策生态的持续完善与优化

**痛点与挑战**

- 从隐私保护立法的整体情况出发，虽然近年来已出台了多部相关法律与要求，但我国隐私法律体系仍处于相对初级的阶段，“摸着石头过河”。
- 聚焦在隐私科技领域，虽然部分国家部委（如发改委）与行业主管机构（如银保监）已出台了一系列的政策，但仍缺乏国家层面整体性的产业政策与指导意见。

**发展方向**

- 法律与政策层面的持续完善，特别是针对数据流通和隐私科技领域的监督与指导意见；
- 针对隐私科技产品，需要逐步建立针对产品本身的设计标准与认证体系，将对用户方选择产品有着极大的指导与促进作用。

## 服务内容和商业模式的持续探索

**痛点与挑战**

- 国内隐私科技产品目前还处于发展的早期阶段，且呈现较为明显的“两级分化”状态：大厂与少数特定行业需求明确且成熟度较高、需求已进化到“隐私计算”领域；大多数行业仍然为满足基本合规要求、“通过Excel解决问题”的阶段挣扎，而这部分需求未得到有效满足。

**发展方向**

- 在满足大多数用户基本需求的层面，可参考国外比较成熟的产品，结合国内用户的痛点与需求，打造中国版的OneTrust；
- 在相对高阶的“隐私计算”层面，探索不同的商业模式，如“跨行业的底层技术与数据平台结合垂直行业的应用平台等等”。

Ethic & Trust

## 技术局限性与用户认知&需求的调和

**痛点与挑战**

主流的PET底层技术如联邦学习、安全多方计算等，都存在一定的局限性：

1）对参与各方特别是用户方的计算能力要求较高；无形中提高了技术应用的门槛与成本；

2）存在应用场景方面的限制；目前主要还是集中在金融、医疗、教育、政务等少数行业。

**发展方向**

- 技术本身的持续优化：特别需要关注，如何降低底层技术的使用门槛与使用成本，进而扩充用户群体；
- 应用场景的扩充，更加契合大多数产于与行业的需求（如零售&快消）。

## 全社会隐私道德意识的提升

**痛点与挑战**

- 求根溯源，隐私保护行业在中国的发展也只经历了不到10年光景；隐私科技更是在最近2-3年才开始“萌芽期”的发展；
- 无论是政府、企业、以及社会大众，其对于隐私与个人信息保护的认知与国外经历了几十年发展的成熟体系相比，还存在较大差距；

**发展方向**

- 国家与政府需要在立法与政策给予持续的支持，同时提升社会大众的认知；
- 用户方（企业）需要严守“道德底线”，在合法合规使用数据的前提下最大化数据的商业价值；
- 厂商从产品与服务设计的角度出发，应该尽可能的满足大多数用户的需求，形成产品与服务的边际效应。

CSA GCR cloud security GREATER CHINA REGION alliance ®

# 谢谢观看！！！