计算机应用行业周报：数据安全 后互联网时代的盛宴

互联网消费升级、强监管时代来临，数据安全已成一种价值主张，产业爆发拐点已至。1）对消费者而言，互联网消费升级时代来临，仅满足使用互联网提供的各种服务的时代已经结束，数据安全将成为一种价值主张，付费意愿提升；2）互联网厂商将在数据安全与商业价值间寻求平衡，随着数据维度与商业模式改变，产业链博弈提升或影响竞争格局，如苹果调整广告标识符（IDFA）政策冲击游戏、广告业务等；3）数据作为新型生产要素，政府天然具备保障公平竞争环境诉求，此外数据共享与保护离不开对安全的立法完善，不论是欧盟 GDPR、还是国内《个人信息保护法》均显示出不能让科技公司以优势地位抢占数据权利定义权的倾向，因为这无法根除“运动员兼裁判员”的隐患；4）随大数据应用发展、政府监管加码与消费者抵制数据滥用，政务、央企、金融及医疗等数据安全需求同样迫切。

数据安全成为互联网监管新内核，《个人信息保护法》、《数据安全法》、《反垄断法》或将构成未来中国互联网监管的三大法律支柱。前者与欧洲《通用数据保护条例》（GDPR）在确保用户隐私的框架上相似，要求国内公司在数据存储和处理方面确保合规性。成本侧，互联网企业将为满足合规要求进行更多的投入，业务侧，原先“数据过度采集”、“消费者价格歧视”等粗放经营漏洞将被打击，用监管力量抵消资本追求非合规收益、超级平台对市场竞争的抑制作用。2020 年《反垄断法》修改将互联网行业纳入考量范围，年末中央工作经济会议提出防止资本无序扩张，2021 年《数据安全法》及《个人信息保护法》等政策实施在即，叠加用户隐私安全意

识加强，互联网厂商数据安全自发需求迫切。

除互联网厂商外，医疗、金融、能源等关保行业数据安全潜在空间巨大。企业侧数据安全需求巨大、有望爆发：1）金融数据天然具有商业价值，需加强监管。通过分析金融交易相关“敏感个人信息”总结、归纳、演绎后得到的“衍生个人信息”，对于风控及业务价值巨大；2）智能医疗设备供应商将收集越来越多样化的数据，其使用必将面临强监管，随实体医院将诊疗活动延伸至互联网端，数据流通成业务刚需，关乎患者隐私、种类繁多的医疗数据也迫切需求安全监管；3）以自动驾驶为代表的 AI 技术日益普及，汽车数据处理量级及能力日益增强，汽车数据依法合理有效利用同时维护了国家安全利益与个人合法权益。

监管政策加码与大数据加速应用驱动数据安全发展，短期百亿市场以技术服务收入为主，长期 SAAS 运营收入有望达千亿。近期《数据安全法》、《关保条例》、《个人信息保护法》等法律法规密集发布并实施，仅从数据安全的组成部分隐私计算来看，据 Gartner 预测，2023 年，全球 80%以上的公司将面临至少一项以隐私为重点的数据保护法规，2024 年隐私驱动的数据保护和合规技术支出将在全球突破 150 亿美元。随《数据安全法》等落地、数据交易市场快速发展，KPMG 预计 2023 年国内数据安全技术服务有望达百亿,随 IT 架构走向云化，长期将撬动千亿级的数据安全 SaaS 运营收入。

竞争格局：典型的数据安全应用场景通常包含三类参与方，互联网作

为数据使用方，相关部门作为监管方，具备良好政治素养、技术储备的第三方企业提供技术服务。以隐私计算场景为例：（1）数据的使用方，需考虑业务特征与支付能力，互联网厂商合规需求迫切，未来数据“最小化采集、避免滥用”，此外如联合建模下的银行业、医疗机构；（2）作为数据的提供方，做到原始数据不出本地，将加密后的信息发送至中间方；（3）数据计算技术服务商，为客户搭建计算系统，包括在业务方、数据方以及可信第三方部署服务节点。考虑国内实际，极可能是由监管单位监管，相关技术储备的第三方企业提供技术服务及运营。

产业机遇：1）卫士通作为数据安全核心公司，参与国家数据安全顶层规划和多项数据安全国家标准制定，具备符合国家合规思路的领先解决方案。基本加密业务信创在手订单充裕，安全芯片等产品军工需求高景气，且成本有望在研究所和上市公司再平衡，净利率预计将显著改善，我们测算 2021 年安全边际市值为 600 亿，2023、2025 年潜在总市值或达 1570.89、3195.93 亿元；2）奇安信前瞻布局的隐私卫士等产品有望核心受益，对应用行为和隐私政策采用可扩展的插件方式进行检测，包括隐私政策完整性检测、与应用行为的实质符合检测、非必要信息收集检测、数