全球数据安全观察

总第 86 期 2022 年第 14 期

（2022.04.18-2022.04.24）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、中央深改委审议通过《关于加强数字政府建设的指导意见》

中共中央总书记、国家主席、中央军委主席、中央全面深化改革委员会主任习近平 4 月 19 日下午主持召开中央全面深化改革委员会第二十五次会议，审议通过了《关于加强数字政府建设的指导意见》。习近平在主持会议时强调，要全面贯彻网络强国战略，把数字技术广泛应用于政府管理服务，推动政府数字化、智能化运行，为推进国家治理体系和治理能力现代化提供有力支撑。

会议指出，**加强数字政府建设**是创新政府治理理念和方式的重要举措，对加快转变政府职能，建设法治政府、廉洁政府、服务型政府意义重大。要把满足人民对美好生活的向往作为数字政府建设的出发点和落脚点；要**以数字化改革助力政府职能转变**；要强化系统观念，健全科学规范的数字政府建设制度体系；**要始终绷紧数据安全这根弦，加快构建数字政府全方位安全保障体系，全面强化数字政府安全管理责任**。

https://mp.weixin.qq.com/s/InDt_EYTD-i1qByB4jJM5g

2、工信部：加快出台《工信领域数据安全管理办法》《APP个人信息保护管理规定》

4月14日上午，国新办举行打击治理电信网络诈骗犯罪工作进展情况发布会，介绍打击治理电信网络诈骗犯罪工作进展情况，并答记者问。针对过度收集个人信息问题，工信部网络安全管理局局长隋静表示，工信部始终高度重视个人信息保护工作，坚决贯彻落实党中央、国务院有关工作部署，坚持以人民为中心的发展思想，立足主责主业，加快推动《个人信息保护法》《数据安全法》在工业和信息化领域落地实施，全面推进**数据安全和个人信息保护**工作取得了积极成效。隋静指出，2022年，工信部还将重点做好以下几个方面工作：一是持续完善管理制度。加快出台《工信领域数据安全管理办法》《移动互联网应用程序个人信息保护管理规定》，**研究制定APP收集使用个人信息、车联网、人工智能等重要领域数据安全标准，强化个人信息保护和数据安全监管**。二是继续开展专项治理。针对涉诈、涉赌、涉网络黑灰产以及疑似恶意程序等不良APP，组织开展APP安全专项治理。建立不良APP安全监测处置技术能力，形成“主动发现、风险预警、依法处置、监管追责”的全流程闭环治理体系。三是保障用户权益。重点突出关键责任链监管，**对应用商店、第三方软件开发工具包、终端企业、重点互联网企业等实现监管全**

覆盖，打造更为安全的信息通信消费环境。四是开展协同共治。我们将加强与网信、公安等部门协同配合，推动构建政府监管、企业自律、媒体监督、社会组织和用户共同参与的综合监管格局，进一步营造更安全、更清朗、更可靠的**个人信息保护和数据安全工作**局面。

https://mp.weixin.qq.com/s/3JZL4Bc37sA2ot7R7HktsQ

3、国家邮政局、公安部、国家网信办联合启动邮政快递领域个人信息安全治理专项行动

4 月 21 日，国家邮政局、公安部、国家互联网信息办公室联合召开电视电话会议，部署开展为期半年的**邮政快递领域个人信息安全治理专项行动**。专项行动小组组长、国家邮政局副局长廖进荣出席会议并讲话。公安部网络安全保卫局政委孙劲峰、刑事侦查局副局长姜国利，国家网信办网络数据管理局副局长方新平对相关工作进行部署。

会议指出，邮政快递业是网络安全和关键信息基础设施保护的重要行业领域，是国家网络安全工作的重要组成部分。本次专项行动一要聚焦解决突出问题，**确保实现涉邮政快递领域侵犯公民个人信息违法犯罪得到明显遏制**，社会公众对邮政快递面单信息保护直观感受明显改善，邮政快递领域信息安全管理短板弱项得到有效补强。二要摸清底数，各企业

要全面开展排查，严格落实人防物防技防措施。三要坚持合成作战，提升打击效能，**对侵害用户信息安全行为“零容忍”**，严厉打击涉寄递电信诈骗、空包“刷单”等违法犯罪行为。四要严格依法监管执法，严肃查处追责，切实形成高压态势。五要加大整治力度，大力推广虚拟安全号码、隐私面单、网络身份认证等技术应用。六要**夯实基础，加强关键信息基础设施安全保护，建立健全网络安全监测预警和网络安全事件应急预案**。

https://mp.weixin.qq.com/s/WKbhaJD12X5cZvDPrkMLoQ

4、《上海城市数字化转型标准化建设实施方案》公布

日前，上海市人民政府官网发布《上海城市数字化转型标准化建设实施方案》（以下简称“《实施方案》”），围绕“经济、生活、治理”全面数字化转型要求，通过研制实施一批能用、管用、好用的数字化转型标准，构建具有系统性、协调性、开放性的城市数字化转型标准体系，为打造具有世界影响力的国际数字之都提供标准支撑。上海市政府披露了数字化转型标准化建设的三大目标：一是构建全覆盖的**城市数字化转型标准体系**，二是构建政府与市场并重的标准供给机制，三是构建适应新发展阶段的标准化工作格局。

《实施方案》明确了数字化转型标准化建设的五大主要

任务，具体包括：完善支撑全局的基础标准、完善融合发展的经济数字化转型标准、完善服务民生的生活数字化转型标准、完善精细管理的治理数字化转型标准、构建适应新发展阶段的标准化工作格局。

《实施方案》要求，完善支撑全局的基础标准。**聚焦城市数字化转型中的基础要素，研制通用基础、数据基座、支撑能力、数字安全、数字信任等标准。**

https://mp.weixin.qq.com/s/iAWRIAAAwExb0trjoNjZlQ

5、《成都市“十四五”数字经济发展规划》发布

近日，《成都市“十四五”数字经济发展规划》（以下简称《规划》）正式印发，系统谋划成都数字经济的五年发展。《规划》以提升**数字技术、数据要素、数字基建**三大数字经济新要素的供给能力为基础，充分发挥智慧蓉城丰富的数字应用场景牵引作用，围绕核心产业引领、新兴产业成势、未来赛道启航的数字经济产业发展体系加快构建，功能引导、场景驱动、优势互补的数字经济区域发展格局加快形成，规范有序、开放协同的数字经济发展生态加快营造，找准成都发展数字经济的动力源和切入点，并明确了任务体系。

https://mp.weixin.qq.com/s/K1jMDFFlzOUpe1kXrarlhg

6、美国《全球跨境隐私规则宣言》（CBPR）发布

4 月 21 日，美国宣布成立“全球跨境隐私规则”体系——Global Cross-Border Privacy Rules System。先前，亚太经济合作组织（APEC）在成员经济体之间设计并发展出了跨境隐私规则（Cross-Border Privacy Rules），而如今的“全球跨境隐私规则”体系，则正是意图将 APEC 框架下的原有体系，转变成一个全球所有国家或者经济体都可以加入的隐私规则体系。声明：1.建立全球 CBPR 论坛，以促进互操作性，帮助弥合对数据保护和隐私的不同监管方法。2.全球 CBPR 论坛的目标是：建立基于 APEC 跨境隐私规则（Cross Border Privacy Rules，CBPR）和处理者隐私认可（Privacy Recognition for Processors,PRP）制度的国际认证体系；通过推广全球 CBPR 和 PRP 机制，支持数据的自由流动、有效的数据保护和隐私；就全球 CBPR 和 PRP 机制相关事宜提供一个信息交流与合作论坛；定期审查成员的数据保护和隐私标准，以确保全球 CBPR 和 PRP 计划要求与最佳实践保持一致；和促进与其他数据保护和隐私框架的互操作性。

https://mp.weixin.qq.com/s/lvmvV2vyaFUUtvB1_Uo0EQ

技术、产品与市场

1、微软推出 Purview 平台来治理、保护和管理敏感数据

随着组织向远程和混合工作的过渡，他们的数字足迹大幅增加，因此微软推出了一套新的解决方案来帮助他们治理、保护和管理他们的整个数据资产。

据称，新推出的 Microsoft Purview 平台集成了 Microsoft 365 合规性和 Azure Purview，并添加了新的功能和产品来帮助管理数据，为企业提供统一的数据治理和风险管理。

新解决方案集可帮助组织了解其整个数据资产中的资产，同时还可以轻松访问其所有数据、安全和风险解决方案。同时，Microsoft Purview 有助于跨云、应用程序和端点保护和管理数据。

https://www.darkreading.com/remote-workforce/microsoft-launches-purview-platform-to-govern-protect-and-manage-sensitive-data

2、Gartner 预测，今年云计算支出将达到 5000 亿美元

根据研究公司 Gartner 的数据，今年全球在公共云服务上的支出将接近 5000 亿美元，到 2023 年将达到 6000 亿美元。云原生基础设施服务的日益普及被认为是关键驱动因素之一，但疫情大流行驱动的混合工作场景的趋势也发挥了

作用。

基础设施即服务 (IaaS) 预计将在 2022 年实现最高的最终用户支出增长，达到 30.6%，作为云堆栈的基础级别，支撑着每一个主要的以消费者为中心的在线产品和移动应用程序。第二高的增长将是**桌面即服务 (DaaS)**，增长 26.6%，因为混合工作促使组织不再使用台式机等传统客户端计算解决方案为员工提供动力。由于对云原生功能的需求，在最终用户支出增长中紧随 DaaS 的是**平台即服务 (PaaS)**，其支出达到 1096 亿美元，比 2021 年增长 26.1%。

随着核心云服务的成熟，提供商之间差异化的重点正在转移到可以直接破坏企业数字业务和运营的能力上。云计算中的新兴技术，如超大规模边缘云计算和安全访问服务边缘(SASE)，正在扰乱相邻市场并形成新的产品类别，进而为公共云提供商创造额外的收入来源。

Gartner 预计，将云与此类新兴技术相结合的组织将在其数字化转型之旅中取得最大成功。

https://www.theregister.com/2022/04/20/gartner_cloud_spending/

3、IDC：2021 年中国 IT 安全软件市场规模达 34.2 亿美元

2022 年 4 月 21 日——IDC《2021 年下半年中国 IT 安全

软件市场跟踪报告》显示，2021 年全年中国 IT 安全软件市场厂商整体收入为 34.2 亿美元（约合 220.4 亿元人民币），较 2020 年增长 31.7%。

IDC 定义的 IT 安全软件市场由**软件安全网关、身份和数字信任、终端安全软件、安全分析和情报、响应和编排软件、其他**，共 6 个功能市场/子市场组成。其中，终端安全软件市场在重点行业大量终端安全新增需求、云工作负载安全（公有云+私有云）快速发展等因素带动下成为 2021 年增长最快的功能市场；因为受到 2021 下半年中国公有云市场增速略微放缓的影响，软件安全网关市场增速相较以往有所降低。

https://www.secrss.com/articles/41584

4、ESG 调查：不能靠支付赎金解决勒索问题！

企业战略集团（Enterprise Strategy Group，简称“ESG”）开展了一项最新调查，研究发现勒索软件团伙在收到企业支付的赎金后，完整归还被盗数据的比例正不断降低。ESG 研究团队表示，支付赎金在很多情况下，会让勒索攻击的后果不断恶化，让勒索软件团伙不断索要另外的赎金。

对北美和西欧地区的 620 位企业 IT 和网络专业人士进行了调查后，数据显示，56%的勒索软件受害者支付了赎金，

以期重新获得对数据、应用程序或系统的访问权。但只有 14.5%的受访者表示实际上拿回了全部数据。研究发现，79%的受访 IT 和网络专业人士表示在去年遭到过勒索软件攻击，17%的受访者声称每周都会面对勒索攻击的威胁。目前，已有 79%的受访者将勒索软件防护列入其业务优先级的前五项。

https://mp.weixin.qq.com/s/Nrmyg0dkf3cX6Crd0mRYig

5、深圳助力建设全国数据交易大市场，196 笔交易覆盖 14 省市

深圳数据交易有限公司（以下简称“深数交”）首批数商及深圳数据交易“2022 数据要素生态圈”计划策划成员 66 家，覆盖全国 14 个省市地区，深数交首批数据商共 62 家，首批数据交易登记备案 196 笔，其中深圳本地数据商数量位居第一，共 17 家，占比 27%，北、上两地数据商分别占比 23%、10%。

据了解，深数交积极探索跨境数据交易。与香港生产力促进局签订“跨境数据流通试点合作框架协议”，推进 8 笔首批跨境数据交易，交易场景覆盖金融、电商、互联网、医疗行业。近期将研究策划跨境数据交易试点和数据海关试点相关工作。

https://mp.weixin.qq.com/s/wL20ec9-zsdgMZKAj9__7g

业界观点

1、周鸿祎：筑牢国家数字安全屏障我们义不容辞

“没有和平的年代，只有和平的国家。坚定的贯彻落实总体国家安全观，是我作为一名在网络安全行业奋战十余年的老兵的使命担当。”4 月 15 日，在第七个全民国家安全教育日这天，三六零（简称“360”）创始人周鸿祎通过微博发文。

他表示，“提到国家安全时，很多人想到的是间谍、特工、战争等，觉得离自己太遥远。但实际上，没有什么岁月静好，数字空间的网络战无时无刻不在发生，只是往往是悄无声息的隐蔽战，大家感觉不到罢了。”

维护国家安全没有谁是旁观者，我们都是国家安全的守护人。周鸿祎表示，“回想当年 360 从美股退市，坚定的选择站在国家和民族利益一边，是无比正确，也无比庆幸的事。尤其当前，国家正处于大力发展数字经济的战略机遇期，360 作为行业龙头企业，为国家筑牢数字安全屏障，护航数字中国建设，维护国家安全，义不容辞”。

https://wlaq.gmw.cn/2022-04/16/content_35667526.htm

2、专家：以互联互通新平台提升数据资源整合效率

在 2020 年下半年，工信部开始启动互联网专项整治行

动，主要解决互联网平台垄断问题，防止资本无序扩张，进而影响到数据资源的市场整合规模和效率。

专家认为，我国目前的数据互联互通政策虽然在部分行业实现了数据融合共享，但与真正的互联互通仍有一段距离，具体表现为：

第一，超级平台的歧视性开放措施依然持续存在，市场割裂问题并未解决。第二，当下互联互通政策以开放链接为主，彼此数据仍不相互流通。第三，互联互通政策仍属于行政指导，缺乏专门立法确认行业规则。

对此，专家建议监管机构应当将数据互联互通视为数字经济发展的基本方向和数据贸易规则的基本原则，按照分步骤、分阶段、分行业的思路逐步推进数据互联互通的基础设备和配套制度的落实进度。

首先，创新监管科技和监管措施，实现专项执法与行政指导的多元共治。其次，明确不同规模平台的特殊义务，结合数据分类分级保护制度，细化数据互联互通制度的基本规则和行业规则。最后，推进数据产权、数据交易等关键性制度供给力度，充分利用北京市科技创新中心区位优势，以技术促融合，以制度保安全，在实现数据互联互通的过程中协调各方利益诉求。

http://www.ciia.org.cn/news/17780.cshtml

3、周小川：数据不动模型动，隐私计算助力数据跨境贸易

4 月 21 日，中国金融学会会长周小川出席博鳌亚洲论坛 2022 年年会时表示，当前的规则和国际协作中，一大难点就在于数据跨境流动和自由交易面临安全、隐私和定价等方面的阻碍。

周小川认为，基于许多国家对数据跨境流动的顾虑，可以考虑不对数据本身进行买卖，而是对数据应用的任务进行贸易。

他谈到安全“隐私计算”的概念，即是在保护数据本身不对外泄露的前提下实现数据分析计算的技术集合，达到数据可用但不可见。在充分保护数据和隐私安全的前提下，实现数据价值的转化和释放。

周小川提到目前科技界普遍重视的一种新技术——“联邦学习”算法。“联邦学习”算法的特征就是数据不动模型动：“如果哪个国家需要另外一个国家的数据，可以把模型委托给联邦学习，让数据保有国的云计算能力进行处理，直接给出最终结果。”

https://mp.weixin.qq.com/s/M8yJZc2GYs6DQxyr7Y1Xag

4、电子报：如何保护个人隐私数据安全？

今年 4 月 15 日是第七个全民国家安全教育日。《电子

报》向作为数据生产及拥有者的个人，提出了四点保护个人隐私数据安全的建议：

守好安全入口。从正规渠道购买手机等互联网终端；购买正规厂商生产的且经过相关部门检测认证的产品；避免被陌生人随意使用；为自己的手机等终端设置一个密码。

定期升级更新软件版本。更新升级版本意味着系统后台增加了更多防范风险的措施，填补了更多系统漏洞，包括对恶意程序的防范、隐私泄露的提醒等。

关闭敏感数据收集权限。设置手机上的应用程序可以拥有什么权限的原则是，应用程序可以拥有合理的权限，关闭过分收集个人信息的权限。

提高防诈意识。相信天上不会掉馅饼，同时不泄露个人隐私数据给陌生人。

https://mp.weixin.qq.com/s/Z9A74kLziOdnXlAe9Mnl9g

5、专家：医疗数据敏感个人信息合规要求高，相关配套细则亟需完善

在疫情的倒逼之下，互联网医疗发展迅速，相关企业的数据合规建设、个人医疗健康信息保护的重要性凸显。据了解，互联网医疗可能涉及包括主诉、患者病史、患者影像数据（CT、MR、PET-CT 等）和健康体检数据在内的多种个人

健康数据。

北京中医药大学法律系教授邓勇教授提到，在互联网医疗场景之中共享个人健康数据时应当确保数据提供者提供的个人健康医疗数据已获得数据主体明确同意。对于共享的个人健康数据，还应当要求数据提供者说明数据来源，并对来源合规合法性进行确认。

此外，多位专家呼吁尽快完善围绕着《网络安全法》、《个保法》、《数据安全法》等法律的配套实施细则。

“应就重要数据及健康医疗数据的识别，在现行法律框架基础上制定具有强制性和可操作性的规范和指南。” 中伦律师事务所律师陈方强提出，执法机关应当对发展现状中存在有关乱象进行预警并采取必要的监管措施。

浙江数字医疗卫生技术研究院战略咨询与研究中心提到，不同场景的数据开放所导致的隐私安全问题不同，因此建立适应于多场景下的隐私安全管理制度与技术保障体系至关重要。可借鉴国外用例管理思路，形成具体场景的数据安全管理指南，为行业落实数据安全和隐私保护提供最佳实践指导。

对于企业及医疗机构而言，中伦律师事务所合伙人蔡鹏提到其应树立合规意识，强化安全管理，落实分类分级制度，积极运用国内外认可的安全技术措施，强化对患者隐私及个

人信息的保护，避免医患纠纷。同时，“强化社会整体的数据保护以及隐私安全意识，将能有效避免数据主体轻易将个人信息泄露的风险。”

https://mp.weixin.qq.com/s/W54SEGqHua3v0WUZLXKGtg

数据安全事件

1、T-Mobile 证实 Lapsus$ 黑客入侵内部系统

2022年4月23日，电信巨头T-Mobile证实，LAPSUS$ 敲诈集团在 3 月获得了对其网络的访问权限。日志显示 LAPSUS$ 集团在 3 月份多次访问 T-Mobile 网络，黑客窃取了多个公司项目的源代码。该团伙从暗网市场获得了初始访问目标系统的 VPN 凭据，然后使用该访问权限执行 SIM 交换攻击。

https://securityaffairs.co/wordpress/130530/data-breach/t-mobile-revealed-lapsus-access.html

2、Conti 勒索软件声称对哥斯达黎加的袭击负责

2022 年 4 月 22 日，Conti 勒索软件团伙声称对袭击哥斯达黎加政府基础设施的勒索软件攻击负责。袭击发生在上周初，它影响了从财政部到劳工部的多个政府部门，而哥斯达黎加政府拒绝支付赎金。至今，Conti 勒索软件团伙已经公布了 50% 的被盗数据。目前尚不清楚这次攻击是否出于政治动机，而 Conti 勒索软件团伙宣布支持俄罗斯入侵乌克兰，哥斯达黎加则公开谴责入侵。

https://securityaffairs.co/wordpress/130505/cyber-crime/costa-rica-conti-ransomware.html

3、未打补丁的 Exchange 服务器遭 Hive 勒索攻击，逾期就公开数据

2022 年 4 月 22 日报道，虽然在 2021 年微软就已针对 Hive 勒索软件发布 Exchange 服务器的安全补丁，并敦促企业及时进行部署，但是依然有一些组织并没有及时跟进。消息称这些尚未跟进的组织近日再次遭受了 Hive 勒索软件的攻击，被黑客获得了系统权限。

在成功入侵后，Hive 进行了一些发现，它部署了网络扫描仪来存储 IP 地址，扫描文件名中含有"密码"的文件，并尝试 RDP 进入备份服务器以访问敏感资产。如果不向 Hive 付款，他们的信息将被公布在 HiveLeaks Tor 网站上。同一网站上还会显示一个倒计时，以迫使受害者付款。

https://www.cnbeta.com/articles/tech/1261193.htm

4、自对俄罗斯发起网络战争以来，匿名者泄露了 5.8 TB 的俄罗斯数据

2022 年 4 月 24 日，据报道，由黑客组织 Anonymous 发起的 OpRussia 网络战行动在超过 5.8 TB 的俄罗斯敏感数据被泄露后继续有增无减。

Anonymous 针对俄罗斯发起的 OpRussia 运动可以看作是对入侵乌克兰的数字反击。该黑客组织声称，大约 5.8 TB

的俄罗斯数据是通过 DDoSecrets 发布的。该组织现在承诺将泄露更多有关俄罗斯企业、组织和政府的数据。他们在信息中强调，他们将俄罗斯商业银行视为优先事项。

https://securityaffairs.co/wordpress/130554/hacktivism/anonymous-leaked-5-8-tb-russian-data.html

5、攻击者利用 DeFi 投票漏洞卷走 Beanstalk 近 1.82 亿美元加密货币

2022 年 4 月 17 日，区块链分析公司 Peck Shield 于上午发布警告称，一名攻击者设法从 Beanstalk Farms 中提取了价值约 1.82 亿美元的加密货币。

攻击者利用通过快速贷款获得的治理令牌组合来创建虚假的协议改进提案，使用该提议赠送存储在 Beanstalk 中的资金。当攻击者从 Stalk 代币获得投票权时，他们可以将所有协议资金转移到他们的个人以太坊钱包中。

https://www.hackread.com/attacker-steal-millions-ethereum-beanstalk-stablecoin-protocol/

7、一公司向境外出售高铁敏感数据每月高达 500G

央广网消息，数字经济已经成为国际竞争的制高点，数据领域面临的国家安全风险日益突出，尤其是国家基础信息、

国家核心数据日益成为境外情报窃密的重要目标。不久前，国家安全机关破获了一起为境外刺探、非法提供高铁数据的重要案件。**这起案件是《中华人民共和国数据安全法》实施以来，首例涉案数据被鉴定为情报的案件，也是我国首例涉及高铁运行安全的危害国家安全类案件**。

上海市国家安全局干警介绍：“境外公司自称其客户从事铁路运输的技术支撑服务，为进入中国市场需要提前对中国的铁路网络进行调研，但是受新冠疫情的影响，公司人员来华比较困难，所以委托境内公司采集中国铁路信号数据，包括物联网、蜂窝和 GMS-R，也就是轨道使用的频谱等数据。” 经鉴定，两家公司为境外公司搜集、提供的数据涉及铁路 GSM-R 敏感信号，GSM-R 是高铁移动通信专网，直接用于高铁列车运行控制和行车调度指挥，是高铁的“千里眼、顺风耳”，承载着高铁运行管理和指挥调度等各种指令。境内公司的行为是《中华人民共和国数据安全法》《中华人民共和国无线电管理条例》等法律法规严令禁止的非法行为。相关数据被国家保密行政管理部门鉴定为情报，相关人员的行为涉嫌《中华人民共和国刑法》第 111 条规定的为境外刺探、非法提供情报罪。

https://mp.weixin.qq.com/s/l9BtRApA4PA83qM225qg4A

8、在线会议 APP 开启静音后，仍在收集麦克风数据

2022 年 4 月 24 日报道，受新冠疫情影响，全球对在线视频会议应用的需求暴涨。近日，研究人员对主流在线视频会议应用进行分析，发现按下静音键后可能并没有静音，应用可能仍然在使用用户麦克风。

当前在线视频会议应用主要基于 iOS、安卓、Windows 和 Mac 操作系统。研究人员对选定 APP 进行了运行时二进制文件分析以确定每个 APP 收集了哪一类数据，以及数据是否构成隐私威胁。研究人员分析发现无论静音的状态如何，所有的 APP 都会定时收集音频数据，除了使用浏览器软件静音特征的 web 客户端。研究人员 APP 收集的数据可以用于进一步分析用户行为。研究人员发现在 82%的情况下可以利用一个简单的机器学习算法对用户按下静音按钮后从麦克风收集的用户数据来成功推测用户行为，包括按键盘、做饭、吃、听音乐、打扫卫生等。

https://mp.weixin.qq.com/s/lOQLI23p8PoFiWPXvGYZKg

9、新的暗网市场 Industrial Spy 正在出售各大公司机密数据

2022 年 4 月 19 日，据报道，威胁参与者推出了一个名为 Industrial Spy 的新市场，出售或向其成员免费提供来自被盗公司的数据。

虽然被盗数据市场并不是新出现的，但 Industrial Spy 并没有以敲诈公司和 GDPR 罚款来吓唬受害者，而是将自己宣传为一个市场，公司可以在其中购买竞争对手的数据来获取商业机密、制造图、会计报告和客户数据库。然而，该市场也有可能被用于勒索，使受害者为了防止数据被卖给其他威胁参与者而进行购买。Industrial Spy 市场提供不同级别的数据产品，其中“高级”被盗数据包价值数百万美元，而较低级别的数据可以作为单个文件以低至 2 美元的价格出售。例如，Industrial Spy 目前正在以 140 万美元的价格出售一家印度公司的高级别数据，以比特币支付。

https://mp.weixin.qq.com/s/leCxTSKgUhmQCSoNRMt5pA

10、数据交易危害国家安全！多家中介公司公开叫卖美军人员信息

2022 年 4 月 22 日报道，研究人员发现，Axciom、LexisNexis 和 NielsenIQ 三家大型数据中介公司均有出售现役或退役军人个人数据的行为；数据经纪公司收集和出售的个人数据范围广、种类多，详细程度堪称“危险级别”，可以轻松用于“人肉搜索”，确认是否属于现役军人；目前美国的数据经纪公司几乎不受监管，可以随意编撰美国公民的个人材料并在公开市场上肆意叫卖，对国家安全来说是一个

巨大的威胁，多位议员呼吁进行监管。

https://www.secrss.com/articles/41642