2022 年 4 月

植德〈国际数据合规热点速递〉

（自 2022 年 4 月 1 日至 2022 年 4 月 30 日）

—植德律师事务所—

北京|上海|深圳|珠海|海口|武汉
Beijing|Shanghai|Shenzhen|Zhuhai|Haikou|Wuhan
www.meritsandtree.com

目录

一、美国篇

1. 美国提出 2022 年医疗网络安全法案

2022 年 3 月 23 日，美国参议员 Jacky Rosen 和 Bill Cassidy 提出了 2022 年医疗网络安全法案（S.3904），该法案将指导网络安全和基础设施安全局 (CISA) 与卫生和公共服务部（HHS）合作，改善医疗保健和公共卫生部门的网络安全。

医疗保健和公共卫生部门掌握着大量敏感的病人信息，并且恶意行为者认为其安全防御很脆弱。针对网络攻击的频率和严重程度加深的情况，公共部门和私营部门开展合作和信息共享，对于提高医疗健康领域的相关实体机构的网络复原力至关重要。

本周早些时候，拜登总统和白宫特别警告美国公司要要根据不断变化的威胁情报，立即采取行动来加强网络防御。根据本周发布的 POLITICO 对 HHS 数据的最新分析，2021 年美国有近 5000 万人的敏感健康数据被泄露，仅在过去三年里就增加了三倍。

【来源：赛博研究院】

2. 美国联邦贸易委员会和伊利诺伊州对大型汽车经销商集团 Napleton 提起诉讼

联邦贸易委员会和伊利诺伊州正在对总部位于伊利诺伊州的大型汽车经销商集团 Napleton 提起诉讼，该集团向客户的账单上偷偷收取不需要的“附加产品”的非法垃圾费，并通过收费歧视黑人消费者他们更多是为了融资。Napleton 将支付 1000 万美元来和解 FTC 和伊利诺伊州提起的诉讼，这是 FTC 汽车贷款案件创纪录的金钱判决。

根据投诉，经销商通常会等到长达数小时的谈判过程结束，才会将附加产品和服务的垃圾费偷偷纳入消费者的购买合同，这些合同通常长达 60 页。尽管消费者特别拒绝了附加组件或确认了不包括附加组件的价格，但这些垃圾费通常会被添加。在其他情况下，消费者被错误地告知附加组件是免费的，或者是购买或资助他们的车辆的要求。

投诉中引用的一项调查显示，83% 的经销商购买者在未经授权或欺诈的情况下被收取附加组件的垃圾费。投诉中引用的一位消费者报告说，位于伊利诺伊州阿灵

顿高地的经销商在他支付了类似金额的首付后，向他收取了近 4,000 美元的附加费。

投诉还称，Napleton 经销商在购买汽车融资方面歧视黑人消费者。Napleton 员工可以通过增加支付的利息金额或在最终合同中添加附加条款来增加消费者贷款的成本。根据投诉，经销商处的黑人客户比类似位置的非拉丁裔白人客户多支付了大约 190 美元的利息，并为类似的附加服务支付了 99 美元。

和解协议还将要求被告建立一个全面的公平贷款计划，其中包括限制他们可以向消费者收取的额外利息加成。和解还要求被告仅在获得明确、知情同意的情况下向消费者收费，并禁止他们歪曲购买、租赁或融资汽车的成本或条款，或者费用或收费是否是可选的。

【来源：FTC】

3. 美国国务院成立网络空间和数字政策局：将新兴技术纳入政策决策

2022 年 4 月 4 日，美国国务院宣布成立其第一个网络空间和数字政策局（CDP），该局强调联邦领域的数字现代化。这是拜登政府的一项关键任务，重点关注国家网络安全、信息经济发展和数字技术三大领域。

目前 CDP 已配备了 60 多名工作人员，其中大多数来自国务院的网络协调和国际通信办公室。国务院计划在今年晚些时候为该局再增加 30 个新职位。当前将以其目前的 60 名工作人员为基础，重点提高对网络外交的认识，以应对类似乌克兰战争、2021 年的微软 Exchange 服务器数据泄露、最近的 Lapsus$黑客攻击以及对 Colonial Pipeline 油气管道的攻击等网络事件。CDP 的网站上写道：“网络空间和数字政策局领导和协调国务院在网络空间和数字外交方面的工作，以鼓励负责任的国家在网络空间行为，并推进保护互联网基础设施的完整性和安全性、服务于美国利益、促进竞争力和维护民主价值观。”

【来源：赛博研究院】

4. 美上诉法院重审可合法抓取能够公开访问的网络数据

美国第九巡回上诉法院，刚刚做出裁定了一项具有里程碑式意义的裁定。过去很长一段时间，某社交软件一直试图通过法律手段，来阻止 Hiq Labs 等竞争对手企业抓取在网络上公开访问的用户信息。该案于去年打到了美国最高法院，但后续又被发回原上诉法院重审。对于档案工作者、学者、研究人员和记者们来说，新

裁定也都具有相当积极的意义。在周一的重申判决中，第九巡回法院维持了原判——认定发现并抓取可在互联网上公开访问的数据，并不违反《反计算机欺诈和滥用法案》（简称 CFAA）。据悉，该法案中规定了构成计算机黑客行为的相关行为。但新裁定为档案工作者、学者、研究人员和记者们使用特定工具，来大量收集或抓取互联网上可公开访问的信息提供了法理依据。

【来源：cnBeta】

5. 美国国会通过《国家网络安全防范联盟法案》

4 月 7 日，美国《国家网络安全防范联盟法案》在参议院获得一致同意，后续将提交总统签署生效。美国国土安全部将很快与国家网络安全防范联盟展开合作，在全美范围内加强网络安全准备与事件响应计划。此项法案授权国土安全部与美国全国大学培训项目联盟等团体合作，共同推动网络安全事件的响应与预防，为各州及地方政府、应急人员、行业利益相关方以及关键基础设施所有者提供跨领域的网络安全培训。根据法案内容，国土安全部将与国家网络安全防范联盟携手，为全美各州、部落及地方政府官员提供技术援助服务与培训。

【来源：安全内参】

6. 某应用商店数十款应用程序秘密收集个人数据，涉及设备超 6000 万台

据 4 月 7 日消息，国际计算机科学研究所和加州大学伯克利分校的研究员 Serge Egelman 和卡尔加里大学研究员 Joel Reardon 在进行安卓应用程序漏洞搜索的审计工作中，发现巴拿马公司 Measurement Systems S.de R.L.编写并植入的软件开发工具包(SDK)代码，能够秘密地获取用户数据。该 SDK 代码最开始被发现于多个下载次数超 1000 万的应用程序中。

研究人员表示，隐藏在应用程序中的 SDK 代码可以获取的数据包括：剪贴板内容、电话号码、电子邮件地址在内的数据。除基于路由器的较粗略位置数据外，还能收集精确的 GPS 数据，并建立数据库，将电子邮件和电话号码与 GPS 历史位置相对应。这意味着，通过这些数据，能在仅知道个人电话号码或邮件的情况下，查询其历史位置信息。

目前，某应用商店已将内置上述 SDK 代码的数十个应用程序下架，其中包括高速公路超速检测应用程序（Speed Camera Radar）、QR 和条形码扫描仪（QR & Barcode Scanner）及简约天气和时钟小部件（Simple weather & clock widget）等。但 Serge Egelman 和 Joel Reardon 发现，尽管自相关信息被曝光后，该 SDK 已停止运行，

没有继续收集数据，但这些代码仍保有从已安装相关应用程序的手机中收集数据的能力。

【来源：数据合规公社】

7. 美国发布“全球跨境隐私规则”宣言

当地时间 4 月 21 日，美国率领一众经济体宣布建立“全球跨境隐私规则”体系——Global Cross-Border Privacy Rules System，并由美国商务部发文。这本质上是将 APEC（亚太经济合作组织）框架下的 CBPRs 体系转变成一个全球所有国家或经济体都可以加入的体系，客观上将推动数据跨境流动，值得跟进关注。

【来源：网安寻路人】

8. Google Play 商店新增数据安全区域：明确收集哪些数据

在去年的博客中，谷歌宣布将为 Google Play 商店推出名为“safety section”的新功能。该功能有助于帮助用户获悉 App 收集的个人数据有哪些，了解到这些数据是否经过加密，同时告诉用户 App 有可能侵犯用户安全和隐私的其它信息。今日，该功能已正式在 Google Play 商店推出，用户将能够确定 App 是否需要数据才能运行，或者数据收集是否可以关闭。

数据安全信息将从今天开始提供，所有开发者都必须在 7 月 20 日之前完成其 App 的隐私信息提交，包括：开发者是否正在收集数据以及出于什么目的；开发者是否与第三方共享数据；该应用的安全实践，例如传输中的数据加密以及用户是否可以要求删除数据；符合条件的应用是否承诺遵守 Google Play 的家庭政策以更好地保护 Play 商店中的儿童；开发者是否根据全球安全标准（MASVS）验证了他们的安全实践。

关于开发者需要披露的更多信息可以在相关页面找到。根据该页面，虚报应用程序的数据收集或未填写该部分，则该应用程序的更新可能被阻止，甚至可能被从 Play Store 中删除。该页面注明：即使是不收集任何用户数据的应用程序的开发者，也需要填写这个表格，并提供其隐私政策的链接。

【来源：IT 之家、cnBeta】

二、欧洲、亚洲、澳洲篇

9. 日本个人信息保护法修正案于 2022 年 4 月 1 日生效

新的个人信息保护法修正案通过扩大日本数据主体的权利范围、强制数据泄露通知以及限制可以提供给第三方的个人信息范围，使 APPI 与 GDPR 更加一致。2020 年修正案于 2022 年 4 月 1 日生效。APPI 适用于在日本处理个人个人数据的所有经营者。这指的是在日本提供商品和服务并位于日本国内的公司和在日本以外设有办事处的公司。因此，与 GDPR 类似，日本的隐私法具有域外效力。但属于其他法规范围的中央政府组织、地方政府、独立行政机构和地方独立行政机构不受 APPI 合规性约束。

【来源：Andrada Coos】

10. 为应对网络攻击，德国风电设备巨头 Nordex 关闭 IT 网络

德国风力涡轮机制造商 Nordex 遭受网络攻击，导致其多地业务部门的 IT 系统被迫关停。Nordex 是一家风力涡轮机设计、销售与制造企业，2021 年全年销售额接近 60 亿美元。Nordex 公司在德国、中国、墨西哥、美国、巴西、西班牙及印度均设有工厂。上周四，该公司称“在早期阶段”检测到入侵活动，并迅速采取了应对措施。在官方声明中，Nordex 公司表示“立即成立了由内部及外部专家组成的事件响应小组，负责遏制问题，阻止进一步传播，并评估潜在风险的具体程度。”“多个 IT 系统关停，可能给客户、员工及其他利益相关方造成影响。Nordex 也将在掌握更多信息时，发布进一步情况更新。”

【来源：安全内参】

11. 欧洲议会通过《数据治理法案》

2022 年 4 月 6 日，欧洲议会就欧盟《数据治理法案》（Data Governance Act；简称“DGA”）进行最终投票表决。最终，《数据治理法案》以 501 票赞成 VS12 票反对、40 票弃权，获得议会批准。根据欧盟委员会的数据，公共机构、企业和公民产生的数据量预计将在 2018 年至 2025 年间增加五倍。基于《数据治理法案》形成的新规则将允许欧盟更好地使用这些数据，预计到 2028 年，通过法案新措施将数据的经济价值提高至 70 到 110 亿欧元，从而使社会、公民和企业受益。

《数据治理法案》旨在促进整个欧盟内部和跨部门之间的数据共享，增强公民和公司对其数据的控制和信任，并为主要技术平台的数据处理实践提供一种新的欧洲模式，帮助释放人工智能的潜力。通过立法，欧盟将建立关于数据市场中立性的新规则，促进公共数据（例如健康、农业或环境数据）的再利用，并在战略领域创建共同的欧洲数据空间。

【来源：数据合规公社】

12. 法国：CNIL 发布人工智能系统 GDPR 合规指南和自我评估工具

法国数据保护机构 ('CNIL') 于 2022 年 4 月 5 日宣布，它已发布了一组关于人工智能 ('AI') 的专用资料。CNIL 特别强调，新资源的发布是在更广泛的欧洲人工智能战略的背景下发布的，旨在为基于人权和基本价值观的人工智能监管框架的发展做出贡献，从而建立欧洲公民的信任。值得注意的是，发布的内容针对三个不同的受众：普通大众；数据控制者和处理者；和人工智能专家。

在对数据控制者和处理者的指导方面，CNIL 特别发布了关于 1978 年 1 月 6 日关于数据处理、数据文件和个人自由的第 78-17 号法案和一般数据保护条例（条例 (EU) 2016/679）（“GDPR”），在基于人工智能系统的个人数据处理实施中将遵循，以及 CNIL 在更具体问题上的立场，包括建立适当的处理法律依据、数据保留期限确定、防范与 AI 模型相关的风险、确保透明度和可解释性以及促进数据主体权利等。此外，CNIL 还发布了 AI 系统自我评估指南。

【来源：OneTrust DataGuidance】

13. 澳大利亚内政部制定《国家数据安全行动计划》

2022 年 4 月 6 日，澳大利亚内政部发布了一份讨论文件，为制定《国家数据安全行动计划》（National Data Security Action Plan，以下简称“《行动计划》”）提供磋商。事实上，早在 2021 年 5 月 6 日，澳大利亚就宣布制定“首个国家数据安全行动计划”，形成国家数据安全框架。这一行动计划也是联邦政府更广泛的数字经济战略的重要组成部分。

《澳大利亚数据战略》（Australian Data Strategy）提出三个主要原则：最大化数据的价值、信任和保护、支持数据使用。《行动计划》则是有关信任和保护的重要措施。为了实现澳大利亚国家数据战略，《行动计划》采取分阶段的方法，加强和协调澳大利亚政府、州和地区政府以及更广泛经济的数据安全政策制定。

【来源：数据合规公社】

14. 英国对在金融服务中使用合成数据征集意见

目前，英国金融行为监管局(FCA)正在寻求了解合成数据在多大程度上可以满足对大量高质量数据日益增长的需求，以帮助开发和培训金融服务部门的创新模型和系统。合成数据是一种隐私保护技术，通过生成统计学上真实的但“人造”的数据，可以为数据共享提供更多的机会。合成数据已经在机器人和自动驾驶汽车等其他领域得到应用，在金融服务领域的探索也处于早期且不断扩大的阶段。通过本次意见征集活动，FCA 希望对市场对合成数据的态度，以及在公司、监管机构和其他公共机构之间开放数据共享的潜力进行初步探索，并且希望了解金融业对合成数据支持创新的潜力和满足企业有效需求的看法，以及潜在的限制和风险。

【来源：未央网】

15. 欧盟数据保护委员会：通过了新的跨大西洋数据隐私框架的声明

2022 年 4 月 7 日，在布鲁塞尔，欧盟数据保护委员会（以下简称“EDPB”）通过了关于宣布新的跨大西洋数据隐私框架的声明。EDPB 支持美国做出的承诺，即在欧洲经济区 (以下简称“EEA”) 的个人数据被传输到美国时采取“前所未有的”措施保护他们的隐私和个人数据，这是朝着正确方向迈出的积极的第一步。EDPB 指出，该公告并不构成 EEA 数据出口商可以将数据传输到美国的法律框架。数据出口商必须继续采取必要的行动，以遵守欧盟法院 (CJEU) 的判例法，尤其是 2020 年 7 月 16 日的 Schrems II 裁决。EDPB 将特别关注该政治协议如何被转化为具体的法律建议。EDPB 期待在收到欧盟委员会的所有支持文件后，根据欧盟法律、CJEU 判例法和 EDPB 先前的建议，仔细评估新框架可能带来的改进，尤其是分析出于国家安全目的收集个人数据是否仅限于严格必要和相称的范围。此外，EDPB 将审查宣布的独立补救机制如何尊重 EEA 个人获得有效补救和公平审判的权利。更具体地说，EDPB 将调查该机制的任何新权力部门在执行其任务时是否可以访问相关信息和个人数据，以及它是否可以通过对情报服务具有约束力的决定。EDPB 还将考虑是否存在针对该当局的决定或不作为的司法补救措施。EDPB 重申，它仍然致力于在保护个人数据的跨大西洋传输方面发挥建设性作用，从而使 EEA 个人和组织受益。

【来源：数据法律资讯】

16. 欧洲数据保护专业公署（EDPS）发布 2021 年度报告

2022 年 4 月 22 日，EDPS 发布了 2021 年年度报告。该报告强调了 EDPS 在欧盟机构（欧盟机构）遵守数据保护框架方面取得的成就。该报告还强调了 EDPS 在倡导在欧盟立法中尊重隐私和数据保护方面的日益重要的作用。

2021 年， EDPS 增加了其纠正权力的使用。在今年 EDPS 采取的执法行动中，特别重要的是命令欧洲刑警组织删除与犯罪活动没有建立联系的数据集的决定，EDPS 认为这是在尊重法治和维护成熟检查的背景下和平衡系统。

就向欧盟立法者提供的 EDPS 建议而言，今年也是前所未有的。EDP S 在 2021 年发布了 88 条意见，包括正式评论，而 2020 年为 27 条，EDPS 解决了创纪录数量的立法咨询。这一增长表明了在欧盟法律中嵌入数据保护的公认重要性。放眼欧盟机构之外，EDPS 还积极保持与民间社会、学术界和其他各种利益相关者的合作。
本着共同负责《通用数据保护条例》成功的精神，EDPS 还继续积极参与欧洲数据保护委员会的工作，提出或参与各种举措。

鉴于全球网络攻击的增加，EDPS 进一步开展工作，提高对个人数据泄露的认识，以协助欧盟机构预防和处理这些事件。近日，法国数据保护机构 CNIL 发布了 2022-2024 年战略计划，专注于以下三个关键主题：鼓励控制和尊重个人权利、将欧盟 GDPR 作为一项值得信赖的资产进行宣传，以及优先针对“高风险隐私问题的监管行动”。CNIL 主席玛丽-洛尔·丹尼斯表示，该计划“应该使 CNIL 能够以灵活的方式与公民、公司、协会和当局一起行动，从而建立一个值得信赖的数字社会。”

【来源：EDPS】

17. 欧盟就《数字服务法案》（DSA）达成正式协议

2022 年 4 月 23 日，欧洲议会和欧洲理事会针对《数字服务法案》达成临时政治协议。《数字服务法案》将为用户提供更安全，更开放的数字空间以及未来几年公司公平的竞争环境设定标准。《数字服务法案》是欧盟委员会于 2020 年 12 月 15 日提交给欧洲议会和欧洲理事会的一项立法提案。法案将迫使科技巨头采取更多措施来处理非法内容，否则将面临巨大额罚款。

此前，欧盟各国和欧盟立法机关就该法案的细节展开讨论，双方在应受法案约束的在线市场平台的定义和禁止定向广告的标准上存在争议。3 月 30 日，鉴于收到

了与欧盟大使会面的授权，欧洲理事会轮值主席国—法国就《数字服务法案》的一些关键问题向其他成员国提出了折衷方案。试图在在未成年人保护、敏感数据、在线市场、大型在线平台的定义以及与系统性风险有关的义务方面与欧洲议会达成一致立场。4 月 23 日，《数字服务法案》经欧洲议会和欧洲理事会达成临时政治协议，有待于理事会和欧洲议会的进一步批准。

【来源：数据合规公社】

特此声明

本刊物不代表本所正式法律意见，仅为研究、交流之用。非经北京植德律师事务所同意，本刊内容不应被用于研究、交流之外的其他目的。

如有任何建议、意见或具体问题，欢迎垂询。

编写合伙人

王艺、陈文昊、龙海涛、吴旸、李凯伦

（执行编辑：深圳办公室 虞晨）

Merits Tree
植德律师事务所

前 行 之 路 植 德 守 护

www.meritsandtree.com