汉坤法律评述
2025 年 11 月 13 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港 | 海口 | 武汉 | 新加坡 | 纽约 | 硅谷

从 ECPA 到 EO 14117：中资公司涉美业务的隐私类集体诉讼风险

作者：段志超 | 刘倩倩 | 金今[1]

2025 年 9 月 2 日，两起针对广告平台的集体诉讼 *Porcuna v. X Inc.*（下文统称为“**X 公司案**”）与 *Baker v. Y Inc.*（下文统称为“**Y 公司案**”）在美国联邦地方法院立案，这是**美国 14117 号行政令（《防止相关国家获取美国人的大量敏感个人数据和与美国政府有关的数据》）及《最终规则》（《防止受关注国家或特定人员获取美国敏感个人数据及政府相关数据的规则》）（下文将美国 14117 号行政令及《最终规则》统称为“EO 14117”）自生效以来首次被美国法院纳入案件审查的情形**。

在这两起案件中，原告指控被告公司违反了 EO 14117，该规则禁止数据经纪商及相关服务提供商将美国人的敏感个人数据出售、转让或以其他方式共享给位于“受关注国家”（包括中国、俄罗斯、朝鲜等）的实体。原告进一步主张，被告公司在违反 EO 14117 的同时，也构成对**《电子通信隐私法案》（Electronic Communications Privacy Act，下文统称为“ECPA”）**的违反。诉状中，国家安全与隐私保护主张被并置提出，显示监管边界正从传统的隐私保护延伸至国家安全维度。

这两起针对程序化广告企业的集体诉讼，被广泛认为是首批以涉嫌违反 EO 14117 为由提起的私人集体诉讼，或将成为美国数据跨境监管与广告科技行业合规实践的重要里程碑。值得注意的是，两起案件创新性地将 ECPA 与 EO 14117 结合，主张广告技术行为若违反 EO 14117 中关于国家安全的数据传输限制，即可被认定为具有 ECPA 第 2511(2)(d)条所界定的“犯罪或侵权目的”。若原告的这一主张获得法院认可，广告科技公司长期依赖的“ECPA 当事方豁免（Party Exception）规则”将不再适用，从而使 ECPA 关于禁止故意拦截的规定直接适用于广告平台。这意味着，原告绕开了对美国司法部执法的依赖，将原本属于国家安全监管范畴的 EO 14117 义务，转化为可在 ECPA 框架下主张高额法定赔偿的民事集体诉讼，为中资公司涉美业务增加了极大的风险。

下文将详细介绍两起案件的基本事实与核心论点。

一、案情事实简介

在 X 公司案中，X 公司作为广告平台，为广告商提供投放工具并与网站和应用开发者合作收集用户数据。X 公司使用 JavaScript 跟踪器、Prebid.js 适配器和 Cookie 同步端点等技术，从用户浏览器获取详细的用户行为数据，包括浏览历史、设备信息、访问页面、Cookie ID、设备 ID 和 IP 地址等。此外，X 公司还能获取上下文信息，例如访问页面的完整链接和引用来源，从而推知用户浏览的具体内容，并获取大量敏感信

[1] 实习生文卓煜、邹昕瑜对本文的写作亦有贡献。

息。

X 公司收集数据后，会使用跨站跟踪技术，与第三方广告公司共享标识符，精准识别访问不同网站的同一用户，并持续追踪其行为。这些信息用于构建用户画像，广告商据此精准投放广告。X 公司还会根据收集的数据形成用户标签，**其中包含敏感分类，如政治倾向、患病信息、性取向、赌瘾等**。某中资海外电商平台是 X 公司数据流的下游接收方之一。在 X 公司平台参与实时竞价时，该中资海外电商平台获得用户行为分组和标识符，帮助其推送定向广告。即使该中资海外电商平台从未直接跟踪用户，这种数据整合也能使其在不同网站和设备之间持续追踪用户。

在 Y 公司案中，Y 公司作为广告平台，通过实时竞价将用户信息（如 IP 地址、Cookie 数据、广告 ID、设备、位置、兴趣、访问页面等）传递给广告商，帮助广告商了解用户浏览习惯和兴趣，做出广告投放决策。

在本案中，Y 公司与某中资海外电商平台等广告商进行数据同步，匹配用户标识符，实现跨平台跟踪。数据交换实时进行，但未获得用户同意。该中资海外电商平台将这些数据与自身跟踪工具结合，分析用户画像。原告称，该中资海外电商平台利用这些数据进行个性化广告投放，甚至可能根据用户的心理或生理脆弱情况推送广告。例如，用户反复查看财务、怀孕或求职相关内容，该中资海外电商平台可能推测用户面临经济压力或处于特定人生阶段。

二、核心论点与法律适用

在论证逻辑上，两案高度相似，均以违反 ECPA 为主要诉由，与此同时创新性地将 ECPA 与 EO 14117 衔接，主张广告技术行为若违反该行政命令中关于国家安全的数据传输限制，即可被认定为具有 ECPA 第 2511(2)(d)条所界定的“犯罪或侵权目的”。依据该主张，广告科技企业将难以继续援引 ECPA 中的“当事方豁免”原则作为其拦截用户通信行为的免责依据。

步骤一：被告行为构成违反 ECPA

ECPA 是一部于 1986 年制定的美国联邦法律，其核心目的在于保护电子通信的隐私，防止其被未经授权的各方拦截或披露。根据 ECPA 第 2511 条，原则上禁止任何人“故意拦截、企图拦截，或唆使他人拦截或企图拦截任何有线、口头或电子通信”。

在 X 公司案及 Y 公司案中，原告均主张被告违反 ECPA，且论述逻辑基本一致，完整拆解了违反 ECPA 的认定要素：

- 首先，被告实施了故意拦截行为。原告主张被告的行为构成了非法的“拦截”。其核心论点是，当用户浏览网页时，被告通过嵌入的代码（如 JavaScript）在数据传输过程中，实时地、未经授权地捕获了用户与网站服务器之间的通信内容，并将这些信息重定向到自己的服务器。这与 ECPA 旨在打击的“窃听”行为在本质上是相符的。
- 其次，原告主张所拦截的信息属于受保护的“通信内容”。原告特别强调，被捕获的内容中包含完整访问 URL，这不仅是一个地址，它直接揭示了用户正在访问的特定页面主题（如糖尿病论坛或宗教经文），从而暴露了通信的实质、目的和私密性，这符合 ECPA 对“内容”的法律定义。
- 再次，原告指出实现拦截的技术工具本身即构成 ECPA 项下定义的“设备”。法律对“设备”的定义十分宽泛，涵盖任何用于拦截电子通信的装置。因此，被告所使用的 JavaScript 跟踪代码、像素标签及 Header Bidding 脚本等，均被论证为属于该范畴内的拦截设备。

- 最后，拦截行为缺乏有效的同意。原告强调，整个拦截过程是在用户完全不知情且未获得其明确同意的情况下秘密进行的。被告既未提供清晰的通知，也未给出有效的选择退出机制。

步骤二：被告行为构成违反 EO 14117 及最终规则

2024 年 2 月 28 日，美国前总统拜登签署了第 14117 号行政命令，指示美国司法部制定法规，以禁止或限制可能导致受关注国家获取美国人大规模敏感个人数据和政府相关数据的交易。2024 年 12 月 27 日，美国司法部发布了《最终规则》，作为第 14117 号行政命令的实施细则，于 2025 年 4 月 8 日正式生效。

从具体适用上，EO 14117 及最终规则约束“美国实体（US Persons）”，并限制其与受限制主体通过进行受限或禁止的交易，以授权受限制主体访问大量美国敏感个人数据或政府相关数据。

在两案中，原告论证被告违反 EO 14117 的核心论点在于：（1）某中资海外电商平台落入“受限制主体”的范畴；（2）被告在“明知”情形下与受限制主体开展“被禁止交易”；（3）某中资海外电商平台获取了大量美国敏感个人数据，可能利用数据优势对美国国家安全构成威胁。

要点 1：某中资海外电商平台落入“受限制主体”范畴

两案中原告均指明，某中资海外电商平台由某中资控股公司运营控制，其在中国运营大量实质业务，并且受中国政府监管。即使该中资控股公司对外公布的官方经营地点位于爱尔兰，其仍受包括《网络安全法》、《数据安全法》、《反垄断法》等法律的管辖，而这些法律要求企业配合政府监管活动提供必要数据。因此该中资海外电商平台属于 EO 14117 意在监管的“受限制主体”。

要点 2：被告在“明知”情形下与受限制主体开展“被禁止交易”

在 X 公司案中，被告主要通过实时竞价，向参与实时竞价的下游接收方提供数据。而在 Y 公司案中，原告指出，被告整合其在 BibleGateway.com 等网站的行为数据，通过原告的某中资海外电商平台关联用户 ID，向该中资海外电商平台提供并传输数据。而根据 EO 14117，以上数据共享行为属于“涉大量敏感个人数据的数据经纪交易”，与此同时不符合任何豁免情形，由此落入“被禁止的交易”范畴。

值得一提的是，两案在起诉状中均重点论证了“明知”要素。两案中的被告均是广告行业重要成员，其所在行业协会深度参与了《最终规则》的制定过程，甚至在规则出台前已明确警告，向中国等“受关注国家”传输行为数据将构成违法，所以被告理应提前知晓，向中国实体传输数据是被明确禁止的。特别地，在 X 公司案中，在规则生效后，其母公司也更新了合同条款以强调合规。然而，X 公司却依然通过其广告系统，持续将美国用户的敏感个人数据（如健康信息、浏览记录和设备标识符）批量传输给受中国法律管辖的某中资海外电商平台。这表明被告并非无心之失，而是在充分了解法律风险和国家安全威胁的情况下，故意维持与受关注实体的数据共享，构成了明知故犯的违法行为。

要点 3：某中资海外电商平台获取了大量美国敏感个人数据，可能利用数据优势对美国国家安全构成威胁

两案中，原告的论述核心是：某中资海外电商平台获取的数据在“量”上是批量的，在“质”上是高度敏感和可识别个人的，在“用途”上存在被用于敌对活动的明确风险，而美国政府的法规已经将此风险认定为现实的国家安全威胁，被告的行为则是明知故犯地为这一威胁铺平了道路。

原告在两案中均强调数据的敏感性和价值。原告指出，某中资海外电商平台通过被告的广告平台系统获取 EO 14117 定义下的“批量敏感个人数据”，包括 IP 地址、广告 ID、设备 ID 和 Cookie 数据。在

X 公司案中，原告指出被告还会捕捉上下文信息及引用来源，暴露其私密内容。被告还会基于收集到的数据形成敏感度较高的分类标签，例如政治倾向、疾病、性取向、赌博癖好等，并通过实时竞价向下游传输，某中资海外电商平台即为参与方之一，有机会获得这些数据。在 Y 公司案中，原告指出被告整合其在 BibleGateway.com 及相关网站的行为数据，收集了他参观的宗教场所、浏览的具体段落以及他可能寻求帮助的问题，并通过原告的某中资海外电商平台关联用户 ID 向该中资海外电商平台提供并传输了这些信息。

在一般语境下，广告技术方收集处理并对外提供的前述信息通常敏感度较低。但在 EO 14117 的影响下，此等数据的敏感度将大幅提高。根据 EO 14117，以上数据均属于“受限制的个人识别信息”，且数量上在《最终规则》生效日期之后已经超过了 10 万，因此落入 EO 14117 定义的“大量敏感个人数据”范畴。

其次，两起案件中，原告均描绘了数据被“武器化”的风险图景。原告主张，在某中资海外电商平台这样一个受中国法律管辖的实体手中，这些数据高度可能不再单纯用于商业营销，而是可以被转化为针对美国的情报和胁迫工具。某中资海外电商平台可以利用这些数据为美国居民（包括法官、军人、记者、政府人员等）建立详尽的个人档案，洞察其生活习惯、健康状况、财务压力和心理弱点。通过分析这些档案，可以识别出处于敏感职位或存在特定脆弱性（如经济困境、隐藏的疾病、非主流政治观点）的个人，对其进行精准定位。这些精准信息可被用于勒索、胁迫、舆论操纵或报复，从而破坏美国关键岗位人员的决策独立性，损害国家安全利益。

最后，原告援引政府权威，将这一行为定性为已知的国家安全威胁。起诉书多次引用美国司法部的观点以及州检察长对某中资海外电商平台的警告和诉讼，强调将美国人的批量敏感数据转移到外国对手手中，本身就被美国政府认定为一种“不寻常且非凡的威胁”。原告指出，被告和某中资海外电商平台的行为，正是美国政府通过 EO 14117 意图阻止的 — 即通过看似合法的商业交易，绕开复杂的网络入侵，直接“购买”能够用于损害美国国家安全和外交政策的数据访问权。

步骤三：被告无法援引 ECPA“当事方豁免”

ECPA 在第 2511(2)(d)条明确了所谓的“当事方豁免（Party Exception）”情形，即：如果通讯的一方当事人参与了拦截，或事先征得了一方同意，那么该拦截行为本身通常不被视为违法。但此“例外”亦有一项关键例外：如果进行拦截的主要目的是为了实施另一项独立的犯罪或侵权行为，那么即使拦截者是通讯一方，其行为亦构成违法。

原告通过结合 EO 14117，创新性地扩张了 ECPA 的适用范围，挑战了广告平台公司长期依赖的当事方豁免。广告平台公司通常以网站代理人的身份部署跟踪器收集数据，并以此为由主张拦截用户通信合法。然而，原告援引 ECPA“犯罪-侵权例外”条款，指出即使拦截者是通信一方，但若其拦截行为主要目的是实施犯罪或侵权，则不适用豁免。原告将被告违反 EO 14117 的行为视为“犯罪或侵权行为”，试图将此新型数据合规与国家安全案件转化为依据 ECPA 提起私人诉讼并寻求高额法定赔偿的传统隐私侵权案件，这将是对 ECPA 适用范围的一次重大突破和测试。

三、影响与建议

这两个案件标志着数据治理领域的范式转变：将常规的商业数据流重新定义为对国家安全的威胁，并利用 ECPA 这一传统法律进行司法追责。它们开创了以违反国家安全法规作为支撑私人诉讼的新策略，一旦成功，不仅会颠覆程序化广告的现有商业模式，更会将中资企业置于数据跨境流动的地缘政治风险之中，迫

使任何涉及美国数据的公司都必须对其数据供应链进行彻底的国家安全审查。数据跨境流动带来的合规风险已从单一的监管应对，扩散至充满不确定性、响应速度更快、且损害赔偿高昂的私人诉讼战场。

- **跨国广告平台合规挑战**

针对跨国广告平台，在诉争应对方面，我们建议不应再单一地依赖 ECPA 的“当事方豁免”条款来为数据拦截行为辩护。取而代之的是，将合规保障前置，通过技术手段实施硬性控制，从而在数据流出企业可控范围之前的初始阶段，就确保其满足 EO 14117 的监管标准。

第三方管理方面，建议严格筛查所有需求方合作伙伴及其最终母公司，确认其是否属于 EO 14117 下的“受关注实体”，建立动态的“受关注实体”清单并实时更新。

协议约束方面，建议在与发布商和广告主的合同中，明确加入合规的陈述与保证条款，并设立强有力的赔偿机制，将法律风险在合作链条中进行明确划分和转移。

在技术隔离措施上，建议对已识别的“受关注实体”实施数据脱敏处理，确保敏感标识符等信息不会通过竞价请求或 Cookie 同步流向这些实体。

- **从广告平台到全行业的 EO 14117 合规挑战**

虽然本次案件的直接被告为广告科技公司，但其实质风险已超越广告领域，任何在业务中处理、访问或间接接触美国人个人数据的企业，无论其行业、所在地或角色，都可能成为潜在合规义务的承担者。因此，本次事件不仅是广告平台的警示，更是所有涉及美国数据流动企业的合规转折点，任何涉及美国用户数据的企业，均需主动建立国家安全维度的数据治理体系，以防范诉讼与执法风险。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com