LINKS Law Offices
通力律师事务所

**上海**
上海市银城中路 68 号
时代金融中心 16/19 楼
电话: +86 21 3135 8666
传真: +86 21 3135 8600

**北京**
北京市建国门北大街 8 号
华润大厦 4 楼
电话: +86 10 8519 2266
传真: +86 10 8519 2929

**香港**
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2592 1978
传真: +852 2868 0883

**伦敦**
1/F, 3 More London
Riverside, London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

**通力法律评述 | 公司及并购**
**2020 年 4 月**

# 不解内忧何以防外患——Zoom 事件的数据合规管理启示

**作者：潘永建 | 邓梓珊**

随着新冠病毒在全球的肆虐，各国相继采取隔离措施，人们纷纷选择 Skype、Teams、Webex 等远程视频会议工具维持正常的工作和社交。在众多的视频会议软件中，Zoom 凭借可容纳大容量用户的优势，成为热门工具，其日活跃用户从去年 12 月份的 1000 万人激增至目前的 2 亿人，甚至不少政府部门使用 Zoom 进行公务会议。然而，近日该款软件接连被曝数据泄漏和安全漏洞问题，引发监管部门和社会各界的广泛关注。本文旨在分析 Zoom 安全事件，总结该事件暴露出的数据合规经验教训，为相关企业提供粗浅合规建议。

## 1. Zoom 安全事件

### 1.1 数据外泄

Zoom 安全事件始于 3 月 26 日，美国科技媒体 Motherboard 指出，Zoom 的 iOS 版客户端内嵌的 Facebook SDK 会向 Facebook 传送用户的手机型号、时区、城市、运营商以及广告唯一标识符等信息。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

除上述与 Facebook 共享用户数据的问题外，Zoom 自身还存在其他安全漏洞。例如 Zoom 的 Windows 版本客户端易受到 UNC 路径注入攻击，这一问题可能导致点击了 UNC 路径链接的用户面临隐私泄露的风险。此外，Zoom 的安全漏洞导致目前至少 15,000 名用户的视频记录在网上被公开。近日，Zoom 还承认，在应对流量上升的过程中，其错误地把用户的会议数据分流到两家位于中国的数据中心进行处理。此次 Zoom 曝出一系列安全漏洞、数据泄露事故，最主要的原因在于未能做到真正的端对端加密。

Zoom 在其发布的声明中表示，内嵌 SDK 与 Facebook 共享的信息不包括参会者个人信息，而是用户设备相关信息，包括操作系统版本、设备时区、磁盘空间、屏幕大小等。但从个人信息的概念出发，当这些设备信息与其他信息相结合，能够识别用户身份，或反映用户活动情况时，也将构成个人信息。个人常用设备信息，包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码等信息也属于通常意义上个人信息的范畴。

Zoom 的一系列安全漏洞存在更多泄露个人信息的风险，甚至是个人敏感信息。例如 UNC 相关的安全漏洞可能导致用户的 Windows 登录密码被窃取，涉及网络身份标识信息；在网络上公开的大量会议视频内容能够显示参会人员的姓名和电话、容貌和声音等，涉及个人基本信息和个人生物识别信息；由于部分视频存在私密谈话和裸露内容，用户个人隐私也因此受到侵犯。

此外，大量政府部门和企业通过 Zoom 进行视频会议，3 月 31 日，英国内阁即在 Zoom 上召开了首场远程会议，英国首相鲍里斯·约翰逊在推特上公开分享了此次会议的屏幕截图。在这些会议中，极有可能涉及大量政府机密或商业秘密事项，在目前已泄露的 Zoom 视频中即可见某公司会议上呈现的财务报表。由此可见，随着 Zoom 视频会议软件的全方位普及，其安全漏洞造成的数据和隐私泄露范围也将愈加广泛。

### 1.2 负面影响

对于 Zoom 而言，其本有可能在疫情期间随着激增的用户需求，迎来快速发展扩张的黄金时期，却由于接连曝光的安全事件遭到用户的抵制。FBI、NASA、SpaceX 或明令禁止员工使用 Zoom，或对于使用 Zoom 的行为提出警告。尽管 Zoom 多次发布道歉声明、采取了修复已知漏洞、宣布冻结新功能等一系列措施也难挡股价连日下跌的趋势。除此以外，已有两名用户在法院向 Zoom 公司提起集体诉讼，分别指控软件“未能保护用户个人信息”和“在未明确通知用户的情况下，收集用户个人信息并与第三方共享”。

Zoom 面临的信任、安全和隐私危机进一步加深，其源头还是在于其内嵌的 Facebook SDK。事实上，Facebook 作为掌握大量用户个人信息、用户使用频率极高的社交平台，Facebook 与其他应用软件的交互能同时为开发者和用户带来便利，很多应用软件都会使用 Facebook SDK。然而 Facebook 也曾多次被曝隐私安全问题，包括卷入剑桥数据分析公司丑闻。此次 Zoom 事件也将淡出公众视线一段时间的 Facebook 数据合规问题再次拉回关注焦点。

## 2. 法律分析

### 2.1 SDK 的“功”与“过”

Zoom 安全事件的主要问题涉及到第三方 SDK 的应用。SDK 全称是 Software Development Kit，即“软件开发工具包”，它是第三方将一些软件功能进行标准化开发后封装成的工具包。只要 APP 安装某款 SDK，便能直接拥有该款 SDK 所具备的标准化功能，这能够极大地提高开发效率、降低开发者成本。目前 APP 开发者使用第三方 SDK 已经成为了普遍现象，APP 接入 SDK 能够快速实现第三方账号登陆、分享、支付、广告、数据统计、地图、风控插件、语言识别、图像识别、推送等一系列常见功能，基本覆盖 APP 开发者的需求。但令人担忧的是，第三方 SDK 在安全性方面通常投入较少，存在多种安全隐患，或是其自身有安全漏洞问题，或是其隐瞒了收集用户个人信息的行为，甚至有部分恶意 SDK 借助合法 APP 实施窃取账号密码、盗刷等侵犯用户个人信息视角下的犯罪行为。

### 2.2 CCPA 视角下的分析

加州消费者隐私法案(California Consumer Privacy Act, CCPA)于今年 1 月 1 日正式生效，该法案旨在加强消费者隐私权和数据安全保护，赋予加州消费者基于收集、使用其个人信息的相关权利，并对在加州开展业务的企业和组织施加了数据保护责任。总部位于硅谷的 Zoom 公司即受 CCPA 监管。

在此次事件中，Zoom 软件内嵌了 Facebook SDK，主要提供第三方账号登录和分享功能。Zoom 在其隐私政策中明确，Zoom 会在用户使用 Facebook 账号登录的情况下收集用户 Facebook 账号相关的个人资料信息，但事实上 Zoom 会将用户使用 Zoom 过程中生产的相关数据共享给 Facebook，甚至包括未使用 Facebook 账户进行登录的用户数据。Facebook 要求使用 Facebook SDK 的 APP 应向用户明确告知“包括 Facebook 在内的第三方可能收集并使用个人信息以提供计量服务或定向广告，但 Zoom 的隐私政策却仅提示 Google Ads 和 Google Analytics 这类第三方服务提供商和广告合作伙伴的自动收集情况，而未明确指出 Facebook 的信息收集行为。另外，虽然 Zoom 发布的更新版本 APP 已移除 Facebook SDK，但 Zoom 并未强制要求现有用户进行 APP 更新或阻止现有用户使用原版本 APP，这意味着若用户继续使用原版本，其用户数据仍将被共享给 Facebook。

根据 CCPA 第 1798.100(b)条[1]和第 1798.110 条[2]，收集和共享消费者个人信息的企业应在收集前向消费者披露个人信息的收集和共享行为、使用个人信息的目的，且消费者有权拒绝企业出售或

[1] 1798.100(b): a business that collects a consumer’s personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

[2] 1798.110(a): a consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following: (1) the categories of personal information it has collected about that consumer. (2) the categories of sources from which the personal information is collected. (3) the business or commercial purpose for collecting or selling personal information. (4) the categories of third parties with whom the business shares personal information. (5) the specific pieces of personal information it has collected about that consumer.

分享其个人信息。Zoom 未在隐私政策中明示 Facebook SDK 收集用户个人信息，即向 Facebook 共享用户使用数据，属于未经告知收集的行为。

此外，Zoom 的多个安全漏洞导致的个人信息泄露也可能违反了 CCPA 第 1798.150(a)条。根据该条规定，若企业未能执行与信息性质相应的合理安全程序和管理措施，而未能尽到保护个人信息的义务，致使未经加密或编辑的个人信息受到未经授权的访问、泄露或窃取，应承担相应的民事责任。[3]

### 2.3 中国法分析

中国法下对于该类安全事件也具有较为完善的法律规定，在中国境内开展相关业务的企业应吸取 Zoom 的教训，在中国法律框架下思考如何降低数据泄露和安全漏洞对企业的威胁。

《网络安全法》作为全面规范网络空间安全管理方面问题的基础性法律，专章规定了“网络运行安全”，要求网络运营者按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。当发现网络产品、服务存在安全缺陷、漏洞等风险时，网络运营者应当履行告知补救、及时处置系统漏洞等安全保护义务。为规范网络安全漏洞报告和信息发布等行为，避免漏洞夸大披露乃至被恶意利用的情况，2019 年工信部发布《网络安全漏洞管理规定(征求意见稿)》专门予以规制。国家及各省市颁布的《网络安全事件应急预案》等规范性文件亦规定了发生数据泄露情形下责任人的报告义务。此外，《信息安全技术 网络安全漏洞管理规范》(征求意见稿)和《信息安全技术 网络安全漏洞分类分级指南》(征求意见稿)等国家标准对数据泄露的预防机制和事后补救义务规定了最佳实践措施，相关从业者可以借鉴参考。

对于个人信息安全问题，《网络安全法》在第四章中明确规定，网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。不得泄露、篡改、毁损其收集的个人信息，未经被收集者同意，不得向他人提供个人信息。根据《数据安全管理办法》(征求意见稿)中的要求，网络运营者对接入其平台的第三方应用，应明确数据安全要求和责任，监督第三方应用运营者加强数据安全管理。《信息安全技术 个人信息安全规范》则更具针对性地提出了可能适用于第三方 SDK 收集使用个人信息情形的“共同个人信息控制者”和“第三方接入管理”的相关规定和要求。此外，《App 违法违规收集使用个人信息行为认定方法》《App 违法违规收集使用个人信息自评估指南》和《信息安全技术 移动互联网应用程序(App)收集个人信息基本规范》均明确要求 APP 运营者应明示 APP 收集使用个人信息的目的、方式和范围，其中包括嵌入的第三方代码、插件。

若企业未能履行网络安全保护义务，侵害用户个人信息依法得到保护的权利，可能受到诸如责令改正、罚款、停业整顿、吊销执照等的行政处罚，而用户也可以依据民法上的相关规定，要求企业承担相应的侵权责任。

[3] 1798.150(a)(1): any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following: …

# 3. 建议措施

## 3.1. 注重法律合规投入

近年来，各类网络安全事件层出不穷，主管部门的执法力度也不断加强，网络安全与数据合规问题几乎成为互联网企业开展业务的生命线。然而，仍有大量企业专注于技术投入，认为只要采购了行业顶尖的技术服务，便能保障网络安全万无一失，而忽视了法律合规体系建设的重要性。事实上，网络安全不仅与技术有关，更与管理相关。近期发生的“微盟删库”事件便是企业需建立完善的内部合规制度的典型例证，微盟因内部运维人员恶意删库，加之安全事故应对经验、准备不足，未能及时恢复数据，导致业务停摆，蒙受重大损失。究其核心原因，还是在于企业对于制度建设、制度的落地实施不重视。如果微盟采取了数据备份措施并确保执行；如果微盟对核心运维人员的权限进行合理设置、限制和制衡；如果微盟定期进行安全事故演练，使运维人员具备了应对数据丢失事件的处理能力，事故是否会发生和发生产生的后果都会大不相同。

因此，预防网络安全事件发生，需要企业内部自上而下树立网络安全与数据合规意识、确立架构完备的合规管理制度并严格遵照执行。从技术角度而言，数据安全风险是难以完全排除的，但法律合规的投入能够有效减小发生网络安全事件的概率。

## 3.2. 完善第三方接入管理

实践中，SDK 能够使用 APP 所申请到的所有操作系统权限，可能存在超出其宣称的功能范围额外收集个人信息的情况。且由于 SDK 数据收集和处理活动缺乏透明度，用户往往难以感知，APP 开发者也未必完全知情。SDK 功能在各类 APP 不同的业务场景下可能收集到多种多样的个人信息。但往往 APP 接入的 SDK 存在问题时，用户首先可能追究 APP 运营主体的责任，因此企业应当加强第三方 SDK 的接入管理。

根据 SDK 不同的个人信息收集方式，第三方 SDK 在法律上的性质有所不同。若 SDK 通过其所依附的 APP 收集个人信息，则视为 APP 收集个人信息并分享给第三方，该种情况下，APP 需在隐私政策中向用户明示第三方 SDK 的名称，以及收集个人信息的目的、方式和范围，当收集个人敏感信息时，更应通过弹窗等方式单独告知第三方的身份和数据安全能力；若 SDK 直接收集个人信息，则其可能自行构成个人信息控制者，或与所依附的 APP 构成共同控制者。但不论属于何种方式，APP 开发者均应在接入前对第三方 SDK 进行安全评估和风险等级评估。在了解 SDK 收集、使用个人信息的具体情况后，通过合同等形式与第三方明确安全责任及相应的安全措施，并向用户明确告知。此外，在第三方接入的过程中也需实时进行监督和审计，发现超出约定的行为应及时切断接入。

## 3.3. 健全网络安全管理措施

冰冻三尺非一日之寒，此次 Zoom 安全事件的发生亦非偶然。早在去年 Zoom 便已暴露了漏洞管理上的不足，当漏洞情况被上报给 Zoom 后，其花了 10 天时间确认漏洞，且在修补漏洞后拒绝公

开细节及提供奖励，Zoom 的漏洞赏金计划沦为形式。Zoom 长期在网络安全与用户数据保护方面的消极应对给其留下安全隐患。

企业应当重视漏洞全生命周期管理，通过完善的内部管理机制和其他漏洞发现渠道，例如企业安全应急响应中心、国家信息安全漏洞共享平台、第三方漏洞提交平台等及时发现、接收和验证潜在安全问题，按要求进行处置、发布和核查，强化企业的安全能力。国家相关法律已经提出了数据分类、重要数据备份和加密等技术措施、管理措施，并制定了详尽的相关国家标准，企业应当严格遵守该类要求并对措施的实施过程进行记录和归档，一方面可以降低安全缺陷、漏洞等问题造成的数据泄露风险，另一方面也可以在真正发生安全事故时尽可能地减轻企业责任。

此外，企业还可以通过与第三方专家和信息安全官的合作，了解网络安全与数据保护领域的最佳实践、探索适用于本企业的最佳技术手段和管理手段。鉴于安全研究人员通常是网络安全事件的发现和曝光者，相关企业也可以适当采用奖励措施、强化漏扫等手段加强与这些专业人员的交流，预防安全事件的发生。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

| 上海 | 北京 | 香港 | 伦敦 |
| --- | --- | --- | --- |
| T: +86 21 3135 8666<br>F: +86 21 3135 8600 | T: +86 10 8519 2266<br>F: +86 10 8519 2929 | T: +852 2592 1978<br>F: +852 2868 0883 | T: +44 (0)20 3283 4337<br>D: +44 (0)20 3283 4323 |

**www.llinkslaw.com**

**Wechat: LlinksLaw**

**本土化资源 国际化视野**