分析 · 2026年5月16日

← 上一页·下一页 →

加密不等于隐私：元数据揭示了您的哪些信息

加密内容与可见的元数据是两回事。当一个服务谈论“端到端加密”时，它只讲述了故事的一半。

并不能保护一切的锁

当今很大一部分即时通信服务都在宣传端到端加密。这是事实：消息内容在传输过程中是加密的，因此路径上的任何人——甚至是服务提供商——都无法在传输过程中读取文本。到此为止，这种说法是准确的。

问题在于，内容只是故事的一部分。虽然没有人能读到您说了什么，但服务商能以极高的精度知道其他事情：您与谁交谈、在什么时间、频率如何、大约在什么位置、使用什么设备、您发送和接收了多少条消息、分享了多少个文件。所有这些都被称为元数据（metadata）。在很多情况下，元数据所透露的信息几乎与消息本身一样多。

元数据揭示了什么

无需阅读消息即可获知很多事情。如果一个人在六个月内，每逢周二早上九点给一位肿瘤科医生打电话或发消息，无需听到对话内容也能猜到发生了什么。如果两个人每天交换一百条消息后突然停止，无需阅读任何一条也能理解发生了什么。如果一名税务顾问在季度结账前夜连续收到来自同一客户的二十条消息，这种模式本身就已经说明了问题。

元数据揭示了行为模式：谁与谁有联系、每个人的日程安排、何时醒来、何时睡觉、何时旅行、哪些客户最活跃、哪些职业关系最紧密。收集元数据的服务器可以为任何用户建立详细的个人和职业生活档案，而无需阅读其撰写的任何一个字。

有一个历史案例严峻地说明了这一点。美国国家安全局（NSA）前局长迈克尔·海登（Michael Hayden）在2014年直截了当地指出：*“We kill people based on metadata（我们根据元数据杀人）”*。该声明指的是美国针对仅凭通信模式识别出的目标进行的军事行动。没有阅读过一条消息。只有联系人图表和时间安排。

服务商收集元数据并不一定意味着它会利用这些数据对付用户。这仅仅意味着它具备这种能力，并且任何能够访问这些数据的第三方——无论是通过法院命令、安全漏洞，还是在服务条款允许的情况下通过出售给第三方——也同样具备这种能力。

对通讯录的访问

另一个几乎被忽视的载体是：联系人列表。很大一部分即时通信服务在注册时要求访问手机通讯录。他们将所有号码上传到服务器，以显示还有谁在使用该服务。从那一刻起，公司就拥有了用户关系的完整图谱，即使该用户从未给任何人写过一条消息。

对于负有职业保密义务的专业人士——律师、医生、心理咨询师、顾问——该通讯录中包含客户。如果通讯录被上传到第三方服务器，客户的名字就处于专业人士无法控制其司法管辖权和政策的底层架构中。职业秘密并非在有人泄露对话之日才被打破：在同意上传的那一刻，秘密就已经被打破了。

“加密”与“不收集”的区别

加密是保护内容。隐私是不收集不需要的东西。这是两回事，其区别在操作层面至关重要。一个服务可以完美地加密所有消息，同时通过元数据几乎掌握用户的一切信息。这两者完全可以共存。事实上，这正是该行业的主流商业模式。

评价一个服务真实隐私性的正确问题不是*“它加密内容吗？”*。这个问题多年前就已有答案。正确的问题应该是：*“它生成哪些元数据，以及这些数据存储在哪里？”*。最重要的是：*“哪些元数据是它原本不需要生成的？”*。

在设计上最大限度减少元数据的架构（privacy by design）——不是靠承诺，也不是靠内部政策——在结构上比收集并加密元数据的架构更具隐私性。因为不存在的数据既不会被泄露，也不会被出售，更不会被移交给法院命令或在安全漏洞中丢失。

致专业读者

如果您的职业活动涉及秘密、机密，或者仅仅是对第三方信息的尊重，那么值得按以下顺序思考这些问题：

1. 我用来沟通的应用程序是否加密内容？（很可能加密。）
2. 它是否加密元数据？（很可能不加密。）
3. 它是否生成了运行所*不需要*的元数据？（几乎肯定生成了。）
4. 这些元数据存储在哪里，受哪个司法管辖区管辖？（很可能在欧洲经济区以外。）
5. 我的客户或患者是否知道其数据存储在那里？

最后一个问题是令人不安的。因为在大多数情况下，诚实的回答是：不知道。

本文是关于专业沟通工具真实运行机制系列文章的第一篇。后续章节将探讨即时通信中的 GDPR 合规性以及数字时代的职业秘密概念。

来源及延伸阅读

- 海登，M. – 2014 年在约翰霍普金斯大学的声明（“We kill people based on metadata”）。公开文字记录可见。
- GDPR（欧盟 2016/679 条例），第 4 条和第 5 条 – 个人数据的定义和处理原则（元数据属于个人数据）。
- 欧洲数据保护专员（EDPS）和 EDPB – 关于电子通信中通信流量数据和元数据处理的意见（ePrivacy 指令）。

← 上一页火漆印章简史下一页 →数字时代的职业秘密

最近阅读

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

随身携带本文，以备不时之需。

↓ Markdown ↓ 纯文本 ↓ PDF

文件将下载到您的设备中。您可以从那里将其保存、导入 Solo2 或在任何地方共享。Cuadernos 不会为您决定文件的去向。

火漆印章 · SHA-256 c18db475ece3522cb204dc052c778b0faee795c006a6c0370b4d852b4c8e65cf

Cuadernos Lacre · Menzuri Gestión S.L. 的出版物 ·
由 R.Eugenio 撰写 · 由 Solo2 团队编辑。