CLOUDFLARE

白皮书

Cloudflare 关于数据隐私和执法请求的政策

发布日期: 2021 年 1 月 28 日

概述

Cloudflare 的网络和业务最终都建立在客户信任的基础上。我们致力于通过构建和部署有助于提高系统安全性的产品、加密静态或传输中的数据，以及允许我们的客户决定如何在全球不同位置检查流量，来不断赢得和维持这种信任。

但并非所有挑战都能通过工程技术来解决。因此，我们也有政策和程序来指导我们如何管理系统上的客户和最终用户数据，以及如何处理政府要求和其他与数据相关的法律要求。

本文简要介绍了这些政策，并就我们在数据隐私和合规方式各方面的详细信息提供了链接。具体包括如下内容：

- 我们有关不断变化的数据隐私形势的观点
- 我们有关数据隐私和数据请求的政策

不断变化的数据隐私形势

云服务的爆炸式增长，以及数据可能储存于数据生成者所在国以外的事实，给各国政府的执法调查构成了挑战。各种各样的在线服务提供商常常充当这些电子记录的接入点。

对于 Cloudflare 这样的服务提供商，政府的数据要求可能令人担忧。执法机构和其他政府部门所做的工作非常重要。同时，执法机构和其他政府部门向我们索取的数据并不属于我们。通过使用我们的服务，我们的客户在数据方面赋予我们信任。维护这种信任是我们业务和价值观的基础。

不同政府在个人数据的保护方面有不同的标准， 这进一步加剧了这种紧张。例如，美国禁止公司披露通讯的内容，包括向非美国政府，仅某些法律规定的情况例外。欧盟 (EU) 长期以来认为隐私是一项基本人权，通过《一般数据保护条例》(GDPR) 保护所有欧盟个人数据。尽管这些保护在某些方面有所重叠，但在范围和保护对象上有所不同。

法律框架之间的差异很重要， 尤其是在判定来自外国政府的数据要求是否符合隐私要求时。例如，近年来，欧盟法院 (CJEU) 在多个场合得出结论：美国对收集数据的法律限制，以及某些自愿承诺（如隐私护盾，或其前身“美国-欧盟安全港”）并不适当地符合欧盟隐私规定，主要是因为美国法律允许执法机构出于获取外国情报目的而收集非美国公民的信息。事实上，欧洲数据保护委员会 (EDPB) 采取的立场是，美国刑法在法律程序以外提出的数据要求（而在该等法律程序中，欧盟国家对所产生的信息拥有一定控制权），并不构成 GDPR 个人数据主体转移的合法依据。

本质上，这些争论的焦点在于：一国政府在什么时候可以使用法律命令或其他法律程序来获取另一国家的公民数据。尽管各个国家对此做出的政策回应并不一致，但现在越来越多国家将获取其公民数据视为国家安全问题。

Cloudflare 关于数据隐私和数据请求的政策

Cloudflare 长期以来一直推行政策来解决对访问个人数据的担忧。我们之所以这样做，一方面是我们认为这是正确的做法，另一方面是我们今天所看到的法律冲突似乎是不可避免的。这些政策包括：

- 有关我们如何处理隐私数据和我们如何处理对该等数据的执法请求的公开承诺
- 我们如何将有关数据请求知会客户。

一般而言，当两种不同的法律标准之间存在冲突时，我们默认选择最能保护隐私的标准。而且我们始终要求遵守法律程序。因为通往数据的大门一旦打开，就难以关上了。

我们有关隐私数据和执法请求的公开承诺

从我们 2013 年详细说明执法请求的首份透明度报告开始，我们就已经就我们处理数据请求的方式做出了公开承诺，就我们从未做过的事情发表公开声明。我们将有关我们从未做过的事情的公开声明称为“金丝雀安全声明”，我们的想法是它们起到向外界发出信号的作用。

这些“金丝雀安全声明”有两个作用。首先，它们是表明我们不会自愿采取这些行动的公开声明。其次，它们可以成为一种传递信息的机制，通过从网站上删除该声明，表明我们已经采取了某些行动（我们可能会被限制以其他方式披露这些信息）。

监管实体已经开始认识到隐私承诺的价值，尤其在承诺可通过合同强制执行时。事实上，多年来我们在透明度报告中所包含的承诺，与欧盟委员会为确保遵守 GDPR 而建议在其《标准合同条款》草案中包含的承诺类型完全一致。

截至本文发布之日，我们所做承诺的主要示例如下：

- **我们从未在我们的网络上安装过执法软件或设备，或提供我们的网络上所传输的内容**：作为安全公司，我们知道，维持对我们网络访问的控制是绝对必要的。因此，我们的安全团队一直专注于访问控制、日志记录和监测，并每年进行多次第三方评估。我们要确保客户能了解，在这些控制中，不存在对执法或政府行为者的任何豁免。因此，我们承诺，Cloudflare 从未在我们网络的任何位置安装过执法软件或设备，我们也从未向任何政府组织提供通过我们网络传输的客户内容源。
- **我们从未共享过加密或认证密钥：** Cloudflare 认为，强加密——包括内容和元数据的加密——对于在线隐私非常必要。如果一个国家希望防止另一个政府获取其公民的个人信息，第一步应当是加密该等个人信息。但客户和监管机构也需要确信，加密本身是值得信赖的。因此，我们承诺，我们永远不会将我们的加密或认证密钥——或我们客户的加密或认证密钥——移交给任何人，我们永远不会应执法部门或任何其他第三方的请求而削弱、降级或破坏我们的加密。
- **我们从未修改过客户内容或 DNS 请求：** 我们认为，我们的系统不应被利用来将人们引导到他们不打算访问的网站，或修改他们在线获得的内容。因此，我们已公开声明，我们从未应执法机构或任何第三方的请求而修改客户内容或修改 DNS 响应的预期目的地。
- **有关潜在承诺违背的透明度：** 我们已承诺挑战任何要求我们违背这些承诺的法律命令，必要时诉诸法庭。我们的目标是，无论是对我们的客户还是世界各国政府，我们的界线都非常明确。

虽然我们有关数据保护的总体理念自创立以来从未改变，我们偶尔会调整承诺，以反映产品和政策环境的最新变化。这些承诺的最终和最新列表请参见透明度报告页面。

将政府请求知会客户

Cloudflare 一直认为，在任何人——包括执法机构或其他政府行为者——使用法律程序来请求客户数据时，客户应当得到通知。在得到通知后，如果客户存在顾虑，就可以挑战该等请求。

事实上，自本公司创立之初，我们就一直有向客户提供通知的政策。2013 年 1 月，我们只有不到 30 名员工时，联邦调查局 (FBI) 带着一封国家安全函出现在我们门前，要求提供一位客户的信息，并禁止我们与律师以外的任何人讨论此事。当时，国家安全函几乎不受任何监管，可由美国政府的单一部门签发和执行，并无限期禁止收件方讨论它们。

我们承认，在某些情况下，执法部门可能需要暂时限制信息披露，以保持调查的可行性。然而，我们也认为，应当要求政府证明任何保密条款的合理性，且任何保密条款都应当明确限制在达到相应目的所需的最短时间内。因此，我们与电子前线基金会 (Electronic Frontier Foundation) 合作，对该信函发起了法律质疑。由此产生的诉讼持续了几年，而且在 2017 年以前我们一直被禁止谈及此事。但到最后，FBI 撤回了该信函。

由于美国法院提出无限期保密命令引发宪法问题，美国司法部于 2017 年发布指引，要求联邦检察人员将保密命令的时间限制为不超过一年，除非有特殊情况。然而，这并未能阻止所有美国执法机构签发无限期保密命令。截至本文发布之日，我们自 2017 年以来已收到 28 份没有结束日期的保密命令。收到此类无限期保密命令时，Cloudflare 都会与美国公民自由联盟 (ACLU) 合作，威胁要提起诉讼。每一次，政府随后都在这些命令的保密要求中加上时间限制，允许我们将有关请求知会客户。

解决法律冲突

要始终遵守 GDPR 等法律，尤其是当所收到的法律命令可能导致我们处于被迫违反此等法律的艰难境地时，需要我们诉诸法院。像 Cloudflare 这样的服务提供商可以因为法律冲突而要求法院撤销法律请求，并且我们在公开声明和数据处理附录合同中都承诺，如果有必要，我们将采取这一措施来避免这种冲突。我们的观点是，这种冲突应当被推回它所属的地方——即争夺信息获取权的两个政府之间。

总结

本文仅介绍了我们在数据隐私方面广泛而深入的承诺。

如需进一步了解这些承诺，请查阅：

- 我们的总体隐私政策：涵盖我们收集什么数据，如何使用数据，共享什么数据，及其他常见的隐私问题。
- 我们的透明度报告：有关我们所收到的披露客户信息法律请求的最新信息。
- 我们的数据隐私与合规主页：有关我们的政策和产品如何支持隐私和合规需求的最新公告。

最后，运营一个保护客户和最终用户数据的全球性网络——并遵守世界各地的不同隐私法律——要求回归到我们公司创立以来所倡导的价值观：坚持原则和透明，尊重隐私，要求合理程序，并知会客户以便后者就其数据自行做出决定。

010 8524 1783 | enterprise@cloudflare.com | cloudflare.com/zh-cn

REV:BDES-5987.2024JUL29