

为什么加密很重要：针对误解的 10 个事实

2021 年 8 月 31 日

在世界范围内，网络攻击威胁着国家安全和民主。这就是加密如此重要的原因：它是在线信任的基础，也是我们确保私人通信和数字基础设施安全的最佳工具之一。然而，面对这些攻击——包括 Pegasus 项目揭露的黑客攻击 [<https://twitter.com/hashtag/PegasusProject>]——政府当局一直在争辩说 [<https://www.politico.eu/article/the-last-refuge-of-the-criminal-encrypted-smartphones-data-privacy/>] 用于加密“后门”，这会破坏互联网的稳定性并使每个人的安全性降低 [<https://www.politico.eu/article/we-need-more-protection-governments-surveillance-not-less/>]。与此同时，苹果公司宣布了一项规避端到端加密的计划 [<https://www.accessnow.org/apple-encryption-expanded-protections-children/>]——这一选择将限制人们对自己设备的控制和危及我们的隐私和安全。

我们的最新报告《政策简报：针对加密误解的 10 个事实》 [<https://www.accessnow.org/encryption-myths-facts-report>] 反驳了我们在过去几年中看到的削弱或绕过加密的最常见论点。它解释了为什么加密如此重要，不仅对于保护隐私、言论自由和其他人权，而且对于支撑经济、维护民主和确保国家安全，也是如此。我们揭穿了最危险的针对加密技术的误解——那些支撑某些法律 and 政策的严重缺陷基础的误解。我们不应该遭受更多的攻击、数据泄露或政治丑闻，让决策者明白为什么加密很重要并且应该受到保护而不是破坏。破坏加密的“安全”政策提案是一种不安全的政策——是时候停止假装不安全了。

事实 1：强大的加密对于互联网安全至关重要

误区：执法后门不会影响我们的权利或民主。（错！）

加密对于数字时代的民主治理以及隐私保护和言论自由权至关重要。通过特殊访问机制削弱加密会危及这些基本人权和整个民主体制。对于某些个人和群体来说尤其必要，包括记者、律师、医生和弱势群体，他们的工作和生活依赖于不受监视的通信渠道的可用性。

事实 3：强加密可增强隐私和安全性

误区：为了实现安全，我们必须牺牲隐私（错！）

将关于加密政策的辩论定义为“隐私与安全”是不准确的，并且是以错误的二元对立思维为前提的。两者是相辅相成的原则。

更合适的辩论框架是“安全与安全”，因为加密不仅保护隐私，还保护安全。这种新构架将有助于确保“安全”政策不会变成“不安全”政策，造成的危险多于它试图防止的危险。

事实 4：执法部门已进入监控的黄金时代——无需破解加密

误区：执法部门正面临“冲破黑暗”的问题，因此有必要破解加密（错！）

“冲破黑暗”的比喻是不准确的。这意味着技术变革在大大扩展时削弱了监视能力。加密没有，也不太可能像政府建议的那样普遍。

对当前时代更准确的比喻是“监视的黄金时代”，因为今天可以获得的个人数据比以往任何时候都多。许多以前未记录的细节，例如位置和联系数据，可以被编译成“数字档案”，描绘出我们日常生活的近距离影像。

事实 5：加密系统的后门不会阻止犯罪分子和恐怖分子使用强加密

误区：削弱加密是打击恐怖主义和犯罪活动的有效措施（错！）

对加密后门的限制的影响是，公众被剥夺了一个保护数据和基本权利的平台。犯罪分子将简单地转向外国司法管辖区或黑市上可用的加密平台，或者他们甚至可能创建自己的平台。

监测能力的提高往往会导致侵入性监测，而没有足够的证据证明其有效性。美国的一项研究表明，提高监视能力与预防恐怖主义之间的联系是微不足道的。无论打击恐怖主义的效力如何，为了识别犯罪行为的部分而危害平台所有用户的隐私和安全是没有必要或不相称的。

事实 6：强大的加密有助于儿童的在线安全

误区：互联网加密技术的使用危害儿童的安全（错！）

与其他犯罪分子一样，针对儿童的犯罪者将转向外国司法管辖区提供的替代加密平台，或创建自己的平台来隐藏他们的活动。这意味着犯罪活动将持续存在 - 它只会超出执法部门的范围，甚至无法合法访问可能有助于调查的元数据。

儿童需要加密平台，在该平台上可以验证与他们交互的个人的身份，并且他们的个人信息不会暴露给第三方。由于新冠全球大流行，随着更多儿童上网，政府和公司应鼓励使用强加密来保护儿童安全，而不是故意在他们使用的技术中引入安全漏洞。

事实 7：强制“可追溯性”将危及隐私和自由表达

误区：必须落实可追溯性，防止虚假信息传播（错！）

可追溯性使匿名性和隐私权面临风险，并对言论自由产生寒蝉效应。因此，它与人权和民主都不相容。

追溯性在实践中的效用有限，不会作为打击虚假信息的有效工具。

事实 #8：强加密对于网络安全和保护国家安全至关重要

误区：对加密内容的特殊访问是保护国家安全所必需的（错！）

强大的加密对于保护国家安全的弹性网络安全基础设施至关重要。破坏加密会危及国家安全。

网络安全事件和有针对性的违规行为的增加是支持而不是反对强加密的论据。没有它，我们将看到更多未经授权的访问和机密信息暴露，这对网络犯罪分子或国家支持的对手来说是一个福音。我们还将看到对医疗系统、选举和公共交通等基本基础设施的更多成功攻击，因为加密系统有助于确保其运营安全。

事实 9：强大的加密可以维持对数字生态系统的信任并支持经济增长

误区：故意破坏加密不会对经济产生影响（错！）

加密是现代数字经济的基石，维护客户数据的机密性和金融交易的真实性。对加密系统的信任会刺激投资、创新和经济增长。

它可以防止或减轻网络安全事件的影响，否则这些事件会造成更大的损害并花费更多的钱。它既降低了数据泄露的风险，又控制了此类泄露的成本，有助于商业利益并支持整个经济。

事实 10：执法和情报机构不必破解加密来调查犯罪

误区：当局别无选择，只能破解加密（错！）

情报和执法机构已经从数字时代个人数据的大量增加中受益匪浅。没有证据表明破坏加密是在现代、尊重权利的民主国家实现政府目标的必要、相称或有效的手段。

在大多数情况下，当局仍然主要依赖传统证据，例如证人、线人、物证以及银行和手机公司的业务记录。破坏加密和削弱每个人的安全性以试图在特定案件中获取所有可能的证据不符合人权和自由，在实践中，永远不能代替良好的调查取证工作。