英译汉

保护用户数据的隐私，防止未经授权的访问，对企业高管、决策者和用户本身至关重要。有针对性的攻击和大规模数据泄露的速度正在加快。每一次新的事件都会损害组织的底线，破坏用户对他们每天使用的产品的信任，并可能对公共安全造成严重后果。问题是多方面的。技术专家正忙于修复软件漏洞。监管机构正努力跟上复杂生态系统的现实。基于市场的方法，如网络安全保险，仍然不成熟。此外，消费者仍在学习他们有什么选择，以及他们应该要求什么选择。目前，最终用户可以使用具有高度确定性的强大隐私保护的软件。不幸的是，这种软件的采用率很低，这主要是因为非专业人士使用起来很困难。事实并非如此。开源社区中的软件开发人员通常是第一个构建加密和隐私工具的人，他们需要改进工具的设计，使其更加用户友好和有用。反过来，公司和政府的购买者应该开始宣传开源软件的价值，尤其是因为它提供了一流的安全性。这些步骤将大大提高在线隐私。

1.背景：密码和用户体验

提供强大隐私保障的工具历来都是利基产品，需要对底层安全机制有特殊了解才能操作它们。然而，许多基本概念都很简单。例如，加密允许对消息内容进行加密，以便第三方无法读取。用户使用类似于长而复杂的密码的加密密钥来加密数据，并使用解密密钥来解密数据。如果用户 Alice 和 Bob 之间传递的消息的加密发生在他们各自的计算机上，并且解密密钥由他们单独控制，则称为端到端加密。这种形式的加密是隐私保护的黄金标准，因为它可以防止潜在的窃听者拦截对话。自 20 世纪 90 年代初，Phil Zimmerman 创建了一个名为 Pretty Good Privacy（PGP）的程序并免费向公众发布以来，用户就可以使用端到端加密的软件工具。然而，非专业用户从一开始就使用这些工具面临着许多挑战。在 1998 年的一篇论文《Johnny 为什么不能加密》中，Alma Whitten 和 J.D.Tygar 记录了 PGP 用户面临的问题。作者发现，参与者甚至难以完成加密和解密消息等基本任务。进一步的研究已经用各种软件程序复制了这些结果。从办公桌到口袋里的手机，将软件融入日常生活，这导致了用户体验（UX）设计的巨大专业化。从大公司到小应用程序开发人员，许多软件公司依靠用户体验的质量生存和消亡，并雇佣大量设计师和研究人员来改善用户体验。毫不奇怪，端到端加密工具在难以使用时受到嘲笑，无论这些工具是用于玩游戏还是秘密谈论敏感材料。考虑到这个行业对用户体验设计的关注，隐私工具仍然以难以理解和使用而闻名，这似乎很奇怪。有几个因素导致了这些明显的缺点，这些缺点限制了用户友好的隐私工具的开发和采用。

2.挑战

隐私保护工具的可用性和采用面临的一个基本挑战是，隐私被视为次要任务，这一点通过用户体验研究得到了证明。在用户心目中，次要任务总是服从于主要任务，这是该软件旨在实现的任何核心活动：在电子邮件客户端中发送电子邮件，在聊天程序中交换即时消息，或在文件共享应用程序中协作文档。许多安全功能都具有这种二等地位：用户将与朋友交谈描述为“安全消息传递”，而仅仅是“消息传递”。这对于软件设计者来说是有问题的，因为如果次要任务变得过于繁重，或者如果他们认为次要任务与主要任务冲突，用户会轻易放弃次要任务的成功。寻求大众吸引力的隐私保护工具面临着另一个重大挑战：非专业用户很难将强大的安全特性与蛇油替代品区分开来。将工具称为“安全”很容易，但如果不在应用商店列表中详细介绍，就很难传达细微差别。多年来，人们一直在努力为安全工具创建第三方批准印章，但这些尝试要么默默无闻，要么缺乏可信度，因为允许开发者在粗略的自我评估后购买批准。创建具有大众吸引力的精心设计的隐私保护工具也面临着各种生态系统障碍。首先，这个领域的大多数工具都是作为开源产品开发的，这意味着作者可以发布源代码供任何人阅读。这对安全性有好处，因为开源开发模型的透明性使得可以对软件进行独立审查（降低关键漏洞的概率）。这对可持续性不利，因为很少有开源项目能够盈利，而且许多项目的资金来源不稳定，如捐赠或赠款。

其次，大多数非专业用户不太可能将他们的数字生活转移到利基安全工具上，他们更喜欢通过选择流行的云平台的便利性来优先处理他们的主要任务。端到端加密与大多数平台采用的商业模式直接冲突，因为它阻止了这些服务的数据挖掘和广告定位。像谷歌这样的服务提供商如果无法阅读电子邮件内容，就无法提供针对性的广告。最后，最近，围绕加密技术的适当性（尤其是与打击恐怖主义或调查犯罪的执法努力相关的技术）进行了几十年的辩论再次兴起，这给软件开发人员带来了巨大的不确定性。苹果和谷歌都进行了升级，以在战略产品（iMessage 的加密聊天、Android 的加密文件系统）中默认支持用户控制的加密。然而，考虑到不同司法管辖区围绕密码学的大量冲突要求即将出现，这些新兴投资不太可能伴随着隐私保护技术的大规模整合。对美国来说，尤其不幸的是，这场辩论出现在对科技公司保护用户数据的能力的信心仍然受到爱德华·斯诺登泄密事件的后果。

3.建议

首先也是最紧迫的是，当前关于加密使用的争论破坏了隐私工具的推广。20 世纪 90 年代初，美国政府利用今天听到的相同论据，提出了与克利伯芯片（Clipper Chip）合作的技术后门。它失败得惊人。尽管此后技术有所发展，但加密的基础却没有。美国和其他国家的政策制定者应该认识到，任何不完整的加密技术都会让所有用户面临风险。开发人员无法构建允许执法人员访问加密通信但阻止恶意行为者利用该访问的软件。密

码学无法区分好人和坏人，所以一个人的后门就是所有人的后门。破坏使用的加密美国公司将使普通消费者面临遭到恶意第三方攻击的风险，并且只会激励犯罪分子和恐怖分子使用多种替代选择中的一种。强大的加密工具可以在美国以外的地方轻松构建；正如自称“伊斯兰国”使用德国通讯服务 Telegram 所表明的那样，软件很少尊重边界。

此外，技术决策者，包括首席信息安全官和其他具有购买力的人，需要在其组织中推广开源工具的价值。这可以通过授权内部工程师在工作时间为开源项目做出贡献，并明确寻求在开源领域有经验的技术顾问来实现。开源开发可以跨越地缘政治障碍，创造出提供一流安全性的技术，但决策者往往认为这些项目是半生不熟的或有风险的。许多项目的志愿作者为这一声誉做出了贡献，但用户体验设计中的不完善造成了更大的损害。从一个客户身上改变一家公司的文化（“软件是一种开支，我能从中得到什么？”）对于其中一个社区（“软件是一项投资，我们如何从战略上为长期利益做出贡献？”）可以帮助组织和项目找到创新、安全且价格合理的解决方案。

反过来，开源开发人员需要优先考虑用户体验研究和设计，并为大型组织优化他们的工具。长期以来，太多项目的焦点都集中在与开发人员相似的用户身上。现在是时候让开源开发的实践专业化了，招募设计师和可用性研究人员加入这项事业，并采取以人为中心的软件设计方法。特别是，项目负责人应通过在其文档中包含对用户体验专家的明确指示，使新参与者更容易了解开发过程。尽管这种焦点的改变需要开源社区的文化转变，但它将使项目吸引更多的用户和更多的捐赠，最终产生更多有用的工具。为了支持这些努力，以技术为重点的基金会和软件公司的研究和开发部门应将资金重点转向更为实用的研究，以制定和交流与安全相关的功能。这一领域的大部分工作都考察了工具难以使用的原因，而不是改进它的方法，或者专注于玩具的改进（例如，“这个自定义界面比标准更好”）。作为此类研究的一个例子，WhatsApp 最近将端到端加密纳入其移动消息平台，而不改变其产品的用户体验。然而，它通过向用户隐藏所有特定于隐私的功能和任务来实现这一点，这反过来又会导致某些类型攻击的漏洞。相反，研究人员应该努力找出使隐私功能在各种工具中成功的因素，并研究如何在不损害用户满意度的情况下将这些功能添加到流行产品中。总之，这些建议将激励和促进组织和个人采取更有力的保护用户数据免受未经授权访问的措施。更容易使用隐私工具和更大的消费者信心反过来将支持数字时代的持续增长、创新和金融稳定。

4.关于作者

Sara“Scout”Sinclair Brody 是 Simply Secure 的执行董事，该组织寻求使隐私保护技术对所有人都有用。Sinclair Brody 长期以来对提高安全工具的可用性感兴趣。她的达特茅斯学院计算机科学博士论文“真实世界中的访问控制”，重点是现代人类组织的经典安全机制。作为谷歌的产品经理，她参与了两步验证和 Android 操作系统等项目。她有撰写了许多关于各种安全主题的学术文章，并共同编辑了《内幕攻击》和网络

安全：超越黑客。外交关系委员会（CFR）是一个独立的无党派成员致力于为其成员提供资源的组织、智囊团和出版商，政府官员、企业高管、记者、教育工作者和学生、公民和宗教人士以帮助他们更好地了解世界和美国和其他国家面临的外交政策选择。成立于 1921 年，CFR 通过保持多样化的成员身份，并通过特别的计划来促进培养下一代外交政策领导人的兴趣和专业知识；召集，召集在纽约总部、华盛顿特区和其他高级城市举行的会议政府官员、国会议员、全球领导人和著名思想家都来了与 CFR 成员一起讨论和辩论重大国际问题；支持促进独立研究的研究计划，使 CFR 学者能够撰写文章，报告、书籍和举行圆桌会议，分析外交政策问题政策建议；出版国际知名期刊《外交事务》事务和美国外交政策；赞助独立工作队，与关于最重要的外交政策议题的调查结果和政策规定；和提供有关世界事件和美国外交政策的最新信息和分析在其网站 CFR.org 上。外交关系委员会在政策问题和与美国政府没有任何关系。其出版物和在其网站上的版权归作者所有。数字和网络空间政策计划解决了 21 世纪最重要的问题之一紧迫的挑战：面对前所未有的挑战，保持全球互联网的开放和安全威胁。通过简报、报告和网络政治博客，该项目的研究员制作及时分析网络空间中最重要的问题。网络简报是简短的备忘录就网络安全、互联网治理、在线隐私和数字商品和服务贸易。