



通讯隐私排名

评估11家科技公司在信息加密
和人权保护方面的状况

概要

加密技术有助于在网上保护人权。通过使数字数据无法阅读，加密技术帮助确保私密信息在互联网传输的私密性，让人们可以在安全的网上空间上网和活动，令他们能没有恐惧地自由发言和表达观点。

加密技术阻止网络犯罪者偷取我们的个人信息，还有助于防止政府非法监控我们的通讯。这对于世界各地的维权人士和记者尤其重要，不论他们是在中国的异议人士，流亡海外的巴林活动人士，还是欧洲的调查记者。若他们的数据安全出现漏洞会损害他们的重要工作，还可能导致他们或其他人被逮捕和拘禁。

科技公司在保护数据信息安全方面起到至关重要的作用。本报告研究了 11 家公司在使用加密技术保护用户的网上安全方面是否履行了其人权责任，并对它们进行了排名。报告特别聚焦于即时通信服务，例如 Skype、WhatsApp 和微信，因为世界各地有数以亿计的人每天都用其进行通讯。

在即时通信服务上进行私人通讯的安全性受到网络犯罪者和恶意黑客的威胁，有关通讯也被国家机关非法拦截。我们依据公司规定的政策和做法，包括它们是否采用有效的加密方式来应对已被确认的人权风险，对公司进行排名。国际特赦组织认为，科技公司必须至少在即时通信服务默认启用端到端加密，即意味着公司本身也无法获取通信内容。

报告中排名最低的公司为黑莓、快拍 (Snapchat) 和腾讯，它们没有在即时通信服务上采用足够的加密强度，令用户的隐私权和言论自由面临威胁。此外：

- 受评估的公司中只有 3 家在其所有的即时通信服务上默认启用端到端加密，包括苹果、连我 (LINE) 和 Viber Media，然而它们中没有一家对于其所采用的加密系统详情充分保持透明性。
- 国际特赦组织发现在 5 起案例中出现政策和做法不一致的情况，例如微软明确承诺保护人权，但在其 Skype 服务上没有采用任何形式的端到端加密。
- 除腾讯外，所有公司都公开表示不批准政府在其通信服务上设置加密后门的要求。

多间受评估的公司公开对维护隐私和安全强烈表示支持，并在面对政府施压时捍卫其加密工具的使用。但即使是排名最高的公司也应做出更多努力，以显示它们在利用加密技术来

应对人权威胁。本报告研究的所有公司也必须就其所采用的加密方式向用户和广大公众展示更透明的态度。

如今承认加密是一项人权问题比以往任何时候都来得重要。政府、科技公司和隐私权倡导者目前正就网上加密工具的使用进行激烈的辩论。有些国家表示担忧，认为通过保护涉嫌犯罪和恐怖主义者的数字数据，加密技术让执法和安全机关无法进行调查，造成被称为“陷入黑暗”的现象。

各国义务保护其人民免遭犯罪侵害，包括恐怖主义。而在遵守国际法的情况下，电子监控可以合法地用于此目的。加密技术确实对执法部门构成挑战，因为就其本质而言，有效的加密技术必须无法被任何人破解，甚至是那些具有合法目的的人。

尽管如此，各国也有义务保护网上隐私权和言论自由，这意味着任何限制或绕过加密的措施必须符合国际法的严格规定。

一些国家如巴基斯坦、印度、土耳其和中国等已经颁布法律，限制取得和使用加密技术。为了处理“陷入黑暗”的问题，一些国家机关建议要求科技公司在加密系统上设置“后门”，为执法部门提供取得被加密信息的特别渠道。

然而，科技专家和密码学者几乎一致认为，不可能设置一套仅供特定国家机关使用的特别接入系统。如果有后门的存在，犯罪者、恶意黑客或其他政府等也将能够使用它。此类措施损害了大多数依赖加密技术来提供保护的人的数字安全，因此在本质上是过度，并不符合国际法的规定。

此外，有关加密技术的争辩正值人们对政府的监控做法增加了不信任之时。爱德华·斯诺登（Edward Snowden）在 2013 年泄露了美国情报文件，揭露英美情报机构如何大规模进行不区分对象的监控活动，以及脸书、谷歌和微软等公司如何面临法院密令要求它们交出客户数据。2016 年 10 月，内部消息来源披露雅虎如何同意美国政府的要求，扫描其所有用户收到的电子邮件。除了大规模监控外，世界各地的政府也利用具有针对性和侵入性的监控工具，在没有合法理由的情况下监视活动人士和记者。

在此背景下，科技公司必须通过为其产品和服务提供有力的数据安全保护，以维护其用户的权利。公司必须抵制政府试图损害或限制使用加密工具的做法，同时在力所能及时满足执法和安全机关提出有关获取信息的合法要求。

在本报告中，受评估的公司大多承认加密技术作为一项工具在保护用户网上安全的重要性。那些公开拒绝政府在其服务系统设置后门的公司如苹果和脸书等应申明加密工具对于在数字世界落实人权至关重要，从而加强其立场；至于那些仰赖较弱的加密技术或没有承认人权风险而落后于同行的公司则必须迎头赶上。

公司排名

国际特赦组织致函所有受评估的公司，要求取得它们目前有关加密标准的信息，以及它们为确保在即时通讯服务方面履行人权责任而制定之政策和做法的详情。我们的评估是根据对公开信息和公司回应（如适用）的分析。

我们以下列 5 项标准给公司排名：

- 公司是否有通过其政策和程序认识到言论自由和隐私权所受到的网上威胁对其用户构成风险？
- 公司是否有默认启用端到端加密？
- 公司是否有让用户了解它们的隐私和言论自由受到的威胁，以及公司如何通过使用加密技术来应对威胁？
- 公司是否有披露关于政府要求取得用户数据的详情，以及公司如何应对此类政府要求？
- 公司是否有公布其加密系统的技术细节？

我们对每项标准最高打 3 分，每间公司可以得到的最高分为 15 分。为便于理解，我们以满分为 100 分的形式给出总分。

国际特赦组织没有评估各即时通信服务的总体安全性，也没有为这里点名的任何应用软件背书认可它们为安全通讯工具。我们建议记者、活动人士、维权人士和任何通讯时尤其可能面临危险的人寻求数字安全专家的意见。

排名	公司	即时通信服务	是否有回复国际特赦组织提出取得信息的要求？	总分（满分为 100 分）
1	脸书	FB Messenger、WhatsApp	是	73
2	苹果	iMessage、FaceTime	否	67
4	电报 (Telegram)	Telegram Messenger	是	67
3	谷歌	Allo、Duo、环聊 (Hangouts)	否	53
5	连我 (Line)	连我 (Line)	是	47
7	Viber Media	Viber	是	47
8	Kakao Inc	KakaoTalk	是	40
6	微软	Skype	是	40
10	快拍 (Snapchat)	Snapchat	是	26
9	黑莓	Blackberry Messenger	否	20
11	腾讯	QQ，微信	否	0

腾讯

腾讯是一家中国互联网公司，开发了微信和 QQ 这两款在中国最受欢迎的应用软件。¹ 腾讯称微信在全球每月有 6 亿 9,700 万活跃用户，QQ 则有 8 亿 5,300 万活跃用户。² 微信是中国最受欢迎的应用软件，不仅用于即时通信，还有商品付款、订货和游戏等多种功能。³

腾讯没有就国际特赦组织提出的信息要求作出回应，也没有公布太多关于处理隐私和其他人权问题的详情。该公司似乎没有在其通信服务中采用有力的加密技术。尽管如此，由于中国法律和条例严格控制互联网，对于中国公司来说采用有力的加密技术可能会在法律和政治上面临很大困难。

2015 年 7 月，公民实验室报告了微信的博客功能如何受到中国政府的言论审查。⁴ 该机构引述的一些报告显示该平台是官方审查的目标，包括言论审查和监控。⁵

标准 1: 公司是否有通过其政策和程序上认识到言论自由和隐私权所受到的网上威胁对其用户构成风险？

国际特赦组织在这项标准上给腾讯的评分为 0。

腾讯对中国国内用户和中国公民实行一套政策，对国际用户则实行另一套政策。此外，微信和 QQ 也有特定政策。

在这两套政策之下，该公司的隐私政策都承诺保护隐私。⁶ 但公司没有承诺保障言论自由，也没有阐明其采取什么行动来保护隐私，仅称“我们使用各种安全技术和程序，以防信息的丢失、不当使用、未经授权浏览或披露”。

¹ 中国互联网观察，《中国 6 大移动社交网络应用软件》，2016 年 4 月 7 日。

² 腾讯，《公司信息》，参见 www.tencent.com/en-us/at/abouttencent.shtml。

³ 《金融时报》，《负超载的中国用户难以应对“微信疲劳”》，2016 年 4 月 16 日。

⁴ J. Q. Ng, 多伦多大学公民实验室，《政治、流言和模糊性：追踪微信公众账户平台的审查》，2015 年 7 月 20 日，参见 <https://citizenlab.org/2015/07/tracking-censorship-on-wechat-public-accounts-platform/>。

⁵ J. Q. Ng, 多伦多大学公民实验室，《政治、流言和模糊性：追踪微信公共账户平台的审查》，2015 年 7 月 20 日，附录：关于微信限制的案例记录。

⁶ 《腾讯隐私政策》（海外），参见 www.tencent.com/en-us/zc/privacypolicy.shtml；针对中国用户和中国公民的腾讯《隐私政策》，参见 www.qq.com/privacy.htm。

腾讯有 5 项公司社会责任承诺，但当中没有任何一项承认对其用户的隐私或言论自由受到的威胁。⁷

该公司没有就我们的来信作出回复，而国际特赦组织也无法找到证据显示该公司有制定任何其他政策和做法，承认与其服务相关的、对隐私权和言论自由的网上威胁。

标准 2: 公司是否有默认启用端到端加密?

国际特赦组织在这项标准上给腾讯的评分为 0。

腾讯对微信实行传输加密，使用户和公司服务器之间的传讯得到加密，⁸ 但没有启用端到端加密。

国际特赦组织无法找到任何应用于 QQ 加密的信息。

公民实验室 2016 年 3 月的一份报告发现，腾讯有另一项叫 QQ 浏览器的网络浏览器服务，它在不加密或仅使用易于解密之加密技术的情况下传输可识别个人身份的数据。⁹

标准 3: 公司是否有让用户了解它们的隐私和言论自由受到的威胁，以及公司如何通过使用加密技术来应对威胁?

国际特赦组织在这项标准上给腾讯的评分为 0。

如上所述，在隐私和言论自由所受的威胁以及对通信服务实施的加密强度方面，腾讯仅对其用户和广大公众提供有限信息。在微信的国际网站上有一个关于安全的常见问题，讲述了一些该服务所采用之加密技术的基本信息。¹⁰ 当用户首次在 QQ 和微信注册时，有一个关于该公司隐私政策和服务条款的链接，但应用软件本身没有关于隐私政策的链接，也没有提到加密技术。

⁷ 腾讯致商业和人权资源中心的信函，2015 年，参见 <https://business-humanrights.org/en/tencent-0>。

⁸ 腾讯，《我在微信上的聊天通信和对话的安全性如何？第三方是否能窃听或读取我的通信？》
<https://help.wechat.com/cgi-bin/micromsgbin/oshelpcenter?opcode=2&plat=1&lang=en&id=1208117b2mai1410243yyQFZ&Channel=helpcenter>。

⁹ J. Knockel、A. Senft 和 R. Deibert，公民实验室，《WUP! 就在那里：QQ 浏览器的隐私和安全问题》，2016 年 3 月 28 日，参见 <https://citizenlab.org/2016/03/privacy-security-issues-qq-browser/>。

¹⁰ 腾讯，《我在微信上的聊天通信和对话的安全性如何？第三方是否能窃听或读取我的通信？》

标准 4: 公司是否有披露关于政府要求取得用户数据的详情, 以及公司如何应对此类政府要求?

国际特赦组织在这项标准上给腾讯的评分为 0。

腾讯的国际版《隐私政策》称, 通过使用其服务“您同意我们或我们的关联公司可能需要保留、保存或披露您的个人资料, 以便 (i) 遵守适用法律和规例; (ii) 遵从法院命令、传召或其他法律程序的规定; (iii) 因应政府机关、执法机关或类似组织 (不论是否位于您的司法管辖区或其他地区) 的要求; 或 (iv) 如我们认为遵守适用法律或条例是合理必需的。”¹¹

腾讯没有就透明性发表报告, 也没有公布其收到的关于取得用户个人信息的特别要求详情。国际特赦组织无法找到腾讯就其服务中设置任何加密后门的事宜所作过的任何声明。

标准 5: 公司是否有公布其加密系统的技术细节?

国际特赦组织在这项标准上给腾讯的评分为 0。

如上所述, 对于微信和 QQ 所应用的加密技术, 国际特赦组织仅能找到有限信息甚至是完全找不到任何信息。

¹¹ 腾讯《隐私政策》(国际版)。

通讯隐私排名

评估11家科技公司在加密和人权保护方面的状况

加密技术有助于在网上保护人权。通过使数字数据无法阅读，加密技术帮助确保私密信息在互联网传输的私密性。

加密技术阻止网络犯罪者偷取我们的个人信息，还有助于防止政府非法监控我们的通讯。这对于世界各地的维权人士和记者尤其重要，不论他们是在中国的异议人士，流亡海外的巴林活动人士，还是欧洲的调查记者。若他们的数据安全出现漏洞会损害他们的重要工作，还可能导致他们或其他人被逮捕和拘禁。

科技公司在保护数据信息安全方面起到至关重要的作用。本报告研究了11家公司在使用加密技术保护用户的网上安全方面是否履行了其人权责任，并对它们进行了排名。报告特别聚焦于即时通信服务，例如Skype、WhatsApp和微信，因为世界各地有数以亿计的人每天都用其进行通讯。

国际特赦组织呼吁所有科技公司在旗下所有即时通讯服务默认启用端到端加密。国际特赦组织认为所有受评估的公司都需要更加透明，表明它们在多大程度上保护用户的网上隐私权和言论自由权。