Atitit 常见加密通讯app

Telegram

**WhatsApp**

**Signal**

一个推荐的就是WhatsApp。Telegram出现前，WhatsApp曾是大众比较看好的一款加密通讯软件，大部分的用户认为 WhatsApp 是安全的。但自从 WhatsApp 被Facebook收购，WhatsApp的安全性就被打上了大大的问号。为啥呢，因为“后爸”Facebook 的生意要想赚更多钱，那就很有可能出于利益考虑，利用WhatsApp 的数据。毕竟数据的金山就放到你面前，唾手可得，换你你能不动心么？

今年4月，WhatsApp宣布在其后版本的软件中，强制启用「端对端」加密（end-to-end encryption）——被视为目前最可靠、安全的加密通讯机制。作为有超过10亿用户的通讯软件，WhatsApp这个改动保障了很多人的通讯私隐。

##### **WhatsApp能保障私隐吗？**

然而在上个星期，WhatsApp修改了其使用条款和私隐政策，将会跟其母公司Facebook分享用户的帐号资料——包括验证用的电话号码，以及跟什么人通讯、通讯时间等「后设数据」（metadata）——以「提高Facebook广告和产品体验」。

批评者指出，WhatsApp在给用户同意更改使用条款及私隐政策的页面上，未有清晰显示这项重要改动。假如用户按下「同意」后才反悔，亦只有30天时间更改设定。更重要的是，用户最多只能拒绝WhatsApp把帐号资料分享给Facebook作「提高Facebook广告和产品体验」等用途，并不代表WhatsApp不会把有关资料交给Facebook。

##### **Telegram也有隐忧**

至于在香港也有不少人使用、主打保密的通讯软件Telegram，其实亦没有其所声称般安全。最大的问题在于，即使Telegram有提供「端对端」加密通讯，但用户必须首先开启其「秘密通话」功能——从这角度而言，Telegram甚至及不上WhatsApp。

此外，Telegram使用自家制的通讯协定，被指未有证明其安全度。美国公民自由联盟（ACLU）的首席技术专家Christopher Soghoian就指出︰「当专家都一致赞扬Open Whisper Systems及WhatsApp使用的Signal协定时，实在没理由使用自己的加密方式——这是电脑保安的基本常识。」

##### **加密通讯软件Signal**

如果真的希望能保障私隐，令通讯内容免遭窃听，在WhatsApp和Telegram以外，其实尚有更多通讯软件可以使用，例如免费的开源软件[Signal](https://en.wikipedia.org/wiki/Signal_(software)" \o "Signal" \t "https://www.thenewslens.com/article/_blank)。

电脑保安专家Moxie Marlinspike曾创立电脑保安公司Whisper Systems，创立了两个加密通讯软件Textsecure和Redphone。该公司其后被Twitter收购，Marlinspike亦因此加入Twitter的资讯安全团队。

其后Whisper Systems把其软件以开放源码方式释出，Marlinspike亦离开Twitter，成立「致力令私人通讯变得简单」的非牟利组织Open Whisper Systems，负责开发和维护一些开源计划，包括结合了Textsecure和Redphone的Signal。

##### **斯诺登推荐使用**

Signal使用的通讯协定获得专家认可，今年4月WhatsApp也是采用其协定，全面改为「端对端」加密。Open Whisper Systems又曾表示，其伺服器上不会储存用户的后设数据，以免泄露用户资料。

而Signal的最佳代言人，应该是揭发美国国安局大规模监控民众的斯诺登（Edward Snowden）。他曾多次赞扬Signal，在[Open Whisper Systems的网站](https://whispersystems.org/" \o "Open Whisper Systems的网站" \t "https://www.thenewslens.com/article/_blank)上更有斯诺登的图片，以及其推荐语︰「使用Open Whisper Systems的任何产品。」