Course: **Privacy by Design and by Default**

Masters Program, EPITA

Class exercise 1b: Tools – **Instant Chatting apps**

Name: Ediz Emektas

Email address: ediz.emektas@epita.fr

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Tool** | | **Opensource**  **/ Proprietary** | **Who owns it?** | **License?** | **Where are they based?** | **Encryption** | **Anonymity** | **What data did you provide/share to acquire that app?** |
| *0* | *Signal* | *Opensource* | *Open whisper systems* | *GPLv3* | *US* | *Yes: end-to-end*  *encryption and*  *Perfect Forward*  *Secrecy* | *No. Open*  *Whisper Systems*  *has access to*  *my GSM no. and contacts.* | *- Downloaded from website (.apk file)*  *- My phone number* |
| 1 | Whatsapp | Proprietary | Facebook | Proprietary | US | end-to-  encryption  protocol | No. Number and contacts shared. (Probably more) | - Downloaded from website or app stores  - Phone number  - ? |
| 2 | Telegram | Opensource | Telegram Messenger Inc. | GNU GPLv2 or GPLv3  (clients) proprietary ([server](https://en.wikipedia.org/wiki/Server_(computing)" \o "Server (computing))) | Germany (2014-2017) United Arab Emirates (2017-) | Yes: end-to-end  encryption and  Perfect Forward  Secrecy | No. It’s possible to hide the phone number from people but the app itself | - Downloaded from website or app stores  - Phone number |
| 3 | Discord | Opensource | Discord, Inc. | Proprietary | US | - | Yes. Can be used with any random nickname | - Only downloaded |
| 4 | Line | Proprietary | Z Holdings | Proprietary | China | end-to-encryption  protocol | Yes. It’s possible to use without phone number. | - Downloaded from website or app stores  - Phone number |
| 5 | Teams | Proprietary | Microsoft | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software)  commercial | US | end-to-  encryption  protocol | No. email address needed and shares with other people | - Only downloaded |

**Q: From your data privacy standpoint, is it safe to use?**

1. Signal

Yes. Because the app does not keep logs to avoid meta-data leakage (except the one’s which are required for operations). My GSM no. and Contact list is hashed on my device, and then stored on their systems to maintain zero-knowledge framework.

1. Whatsapp

Not as much as Signal and Telegram. Keep logs by default and uploads to data center whenever the phone connected to wi-fi.

1. Telegram

Yes. It encrypts all the data end to end. Also, possible to use with an anonym account. Secret kind of chats are possible too, which gives opportunity to delete messages after a while.

1. Discord

Yes. Discord is generally a safe social platform. So long as you don’t join any really toxic servers or act foolishly around predatory people, you’re generally safe.

1. Line

As safe as Whatsapp, because of using same kind of encryption system with slightly different kind of anonymity. It wouldn’t be my first choice but most of the Asian people trust its environment.

1. Teams

Yes. As far as only authorized users can access your organization’s Teams platform, it’s safe to use.