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

Masters Program, EPITA

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

Name:

Email address:

**THIS IS AN TEMPLATE FILE – DO NOT CHANGE (i.e., DOWNLOAD AND USE)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 | … | … | … | … | … | … | … | … |
| 2 | … | … | … | … | … | … | … | … |
| 3 | … | … | … | … | … | … | … | … |
| 4 | … | … | … | … | … | … | … | … |
| 5 | … | … | … | … | … | … | … | … |

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

0: 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.

…

2.

…

3.

…

4.

…

5.

…