Course: **Privacy by Design and by Default**
Masters Program, EPITA
Class exercise 1b: Tools – **Instant Chatting apps**

Name: Haozhe TANG
Email address: haozhe.tang@epita.fr

THIS IS A 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	Telegram	Opensource	Telegram Messenger Inc.	GPLv2 or GPLv3	Dubai, United Arab Emriates	Yes: end-to-end encryption and MTProto	No. Should access to my GSM no. , SMS, phone call logs and contacts	-Downloaded from app store(.apk file) -Phone number -name and profile(Can be nickname)
2	Wechat	Proprietary	Tencent	Proprietary freeware	Shenzhen, China	No: no specific encryption method for now.	No. Should access to my GSM no. , SMS, phone call logs and contacts	-Downloaded from app store(.apk file) -Phone number -name and profile(Must be real name) -ID identification
3	Skype	Proprietary	Microsoft	Proprietary	Luxembourg	Yes: end-to-end encryption	No. Should access to my email, phone call logs, postal mail and contacts	-Downloaded from app store(.apk file) -email -postal mail -notifications -microphone -camera
4	Dingtalk	Proprietary	Alibaba Group	Proprietary freeware	Hangzhou, China	Yes: SSL/TLS security standards.	No. Should access to my GSM no. and SMS	-Downloaded from app store(.apk file) -Phone number -camera -microphone
5	Whatsapp	Proprietary	Meta Platforms, Inc.	Proprietary software with EULA	California, US	Yes: end-to-end encryption	No. Should access to my GSM no. , SMS, phone call logs and contacts	-Downloaded from app store(.apk file) -Phone number -name and profile(Can be nickname) -microphone

Q: From data privacy standpoint, is it safe to use? (please also check the application score, given by Exodus)

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:Telegram

Yes. Because the text, audio and video chats are all encrypted by end-to-end encryption. As for the cloud chats, they are encrypted between the app and the server, which makes SPs and other third-parties on the network can't access to the data, but the Telegram server can. Besides, it provides a specific "secret chat" for users, which be sent with client-to-client encryption and these messages are encrypted with the service's MTProto protocol. At last, this app does not have any trackers, which minimize the chance to leak users' information, and the permissions it requires are the ones must be acquired if users want to use all the functions. All in all, the messages we sent are not easy to get leaked.

2:Wechat

Not really. First of all, there is not a specific encryption method for the data we have given or we produce during the usage of it, so the data itself is easy to be leaked during the transfer. Besides, this app has 5 trackers to collect the information. What's more, some permissions are unnecessary, for example: WRITE_SETTINGS.

3:Skype

Yes. Skype provides end-to-end encryption, which protect our messages. As for the aspect of trackers, it has only two trackers which are helping the app to detect and analyze crashes. And the permissions it requires are the ones must be acquired if users want to use all the functions.

4:Dingtalk

Yes. Firstly, this app can be the communication system directly by companies because it has every function might be used in running a company. So, at company level, Dingtalk encrypts messages and files at SSL/TLS security standards which can confirm the safety between the sender and receiver. Besides, it becomes the edge tool during the pandemic for Chinese students to attend class online. All the videos recorded on the platform are encrypted by RSA and other more complicated encryptions, making the videos can only be seen by users specifically.

5:Whatsapp

Yes. This app has only one tracker which helps to detect and analyze crashes. As for the permissions, it will ask for users' permission if they want to use the specific function, if user do not agree with that, it will not work. Whatsapp adds end-to-end encryption in 2016. Besides, Whatsapp's developing group discovered several bugs and some functional flaws every year, it makes this app to enhance its security level higher and it exists less possibility for leaking information.