



Lancaster University College  
at Beijing Jiaotong University

# Group 8

## Group Member List:

Miao Cai 16722043

Zhuohua Qi 16722019

Chenhui Mao 16723026

Haotian Sang 16722022

# Privacy Presentation Outline

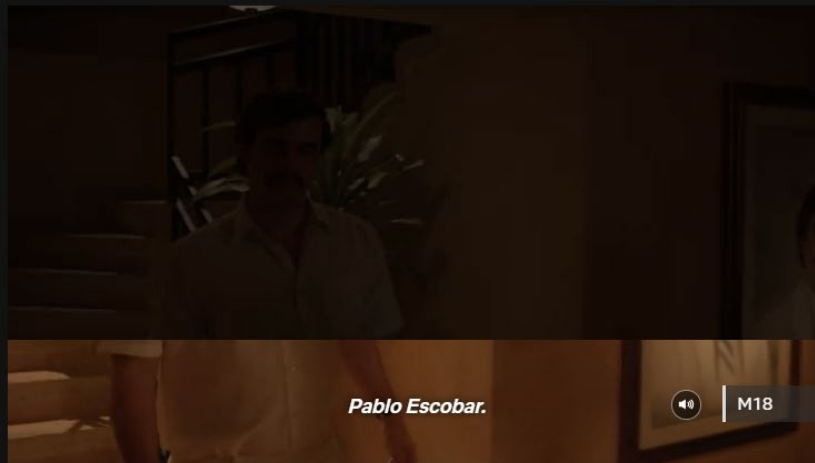
- Brief summary of the Netflix Inc.
- Privacy policy study of the Netflix Inc.
  - Collection of Information
  - Access to Account and Profiles
  - Changes to This Privacy Policy
  - Use of information
  - Disclosure of Information
  - Children Policies
- Brief summary of the Tencent Inc.
- Evaluation of the Tencent privacy policy
  - Register
  - Social network
  - Minor protection
  - Missing privacy protections

# WHY DO WE CHOOSE **NETFLIX**?

## Netflix Originals



## Trending Now



NETFLIX ORIGINAL

## NARCOS

▶ Play

✓ My List

First they got the coke. Then they got the money. Now the Colombian cartels want the power. Let the drug wars begin.

# N ABOUT NETFLIX

*“Netflix has been leading the way for digital content since 1997, the world's leading internet entertainment service with over 148 million paid memberships in over 190 countries.”*

*– The Netflix Media Center*

Name: Netflix

Web address: <https://www.netflix.com>

Type of site: The subscription-based online streaming video website

- Identities:
1. The most popular streaming service in the world
  2. Has to comply with **laws** of different countries and handle the various government **requests**.
  3. Related to **race**, **ethics**, **crime** issues
  4. Maturity rating & parent control

Little Kids	Older Kids	Teens	Mature	Restricted
G	PG	PG-13	M18, NC16	R21

Source: <https://help.netflix.com/en/node/2064>



# SUMMARY

## Summary

Netflix, as one of the most popular streaming video websites that owns millions of members over 190 countries, has written its own privacy policy to comply with various laws and government requests and clearly expressed its position on member's privacy.

However, some privacy statements are unclear or unreasonable, which in turn lead to race, ethic and crime issues and may possibly break the children protection laws.



# CLEAR POLICIES

## Collection of Information

- List general methods to collect the information
  - e.g., Cookies, web beacons and other technologies.
- List in detail which information will be collected
  - i.e., IP address, referral URLs, device IDs, phone number, etc.





# UNREASONABLE POLICIES

## Access to Account and Profiles

- *A right to be forgotten* is not clear
  - No mention of delete related history/cookies policy.
  - Deactivation duration is unreasonable

## Changes to This Privacy Policy

- **Do not** notify the updates to the members **but** enforce terms



# USE OF INFORMATION

## CLEAR VS. UNCLEAR

- Detect and investigate illegal activities
  - i.e., Payment fraud, etc.
- Provide localized content
- Send news or consumer surveys
- Optimize recommendation algorithms
- Assist with operational requests
  - e.g., Password Reset
- Anticompetitive (free ride)
  - Violate the member's right to know.
  - Gain money for another big money by making Netflix originals.
- Privacy abuses
  - Recommendation based on race (especially to African Americans).





# DISCLOSURE OF INFORMATION

## REASONABLE VS. UNREASONABLE

- Describe certain purposes
  - e.g., Promotional offer, business transfer and legal right protection of Netflix and others
- Member does not realize what kind of information is connected with Service Providers.
  - Violate the ***right to know***
- Member has no right to decide whether or not to make a consent
  - Also lack of providing ***opt-in*** policy
- Do not take responsibility for the ***consequence*** of the third parties use of information
- Disclosure of member's watching history to the third party violate the ***Video Privacy Protection Act***



# CHILDREN POLICIES

## CLEAR VS. UNCLEAR

- Apply informed consent for both adults and children.
  - e.g., Children could only watch the Netflix under the approval of a parent or legal guardian.
- Use of children information is not clear yet.
  - Maybe disobey the ***Children's Online Privacy Protection Act***

# WHY DO WE CHOOSE

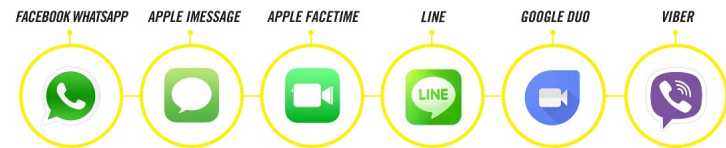


# QQQ ?

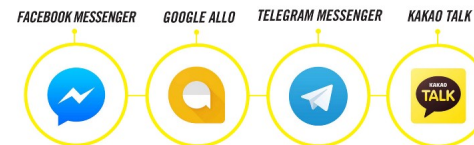
COMPANY	IM SERVICES ASSESSED	1. RECOGNISES ONLINE THREATS TO HUMAN RIGHTS?	2. DEPLOYS END-TO-END ENCRYPTION AS A DEFAULT?	3. INFORMS USERS OF RISKS AND ENCRYPTION USED?	4. DISCLOSES GOVERNMENT REQUESTS FOR USER DATA?	5. PUBLISHES TECHNICAL DETAILS OF ENCRYPTION?	OVERALL SCORE /100
FACEBOOK	FB MESSENGER, WHATSAPP	Yes, but only committed to freedom of expression through participation in multi-stakeholder initiative. Score 2	Yes, but only on WhatsApp, not on Messenger. Score 2	Inadequate notification within the apps, no warning in Messenger when using weaker encryption. Score 1	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. Score 3	Yes, both apps use open source Signal protocol, provide specification. Score 3	73
APPLE	IMESSAGE, FACETIME	Yes, but no policy commitment to freedom of expression. Score 2	Yes. Score 3	Inadequate notification within the apps. Score 1	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. Score 3	Some specification of encryption, but protocol not open source. Score 1	67
TELEGRAM	TELEGRAM MESSENGER	Yes, stated commitment to rights and recognition of online threats. Score 3	Has end-to-end encryption, but not set as a default. Score 1	Inadequate notification within the apps, no warning when using weaker encryption. Score 1	Commitment not to share user data, but no transparency report with details of requests received. Has taken public stance against encryption backdoors. Score 2	Yes, app is open source, although implementation unlicensed. Score 3	67
GOOGLE	ALLO, DUO, HANGOUTS	Yes, but only committed to freedom of expression through participation in multi-stakeholder initiative. Score 2	Yes on Duo, but only as an option on Allo, Hangouts not at all. Score 1	Inadequate notification within the apps, no warning when using weaker encryption. Score 1	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. Score 3	Allo uses open source Signal, but not published specification yet. Score 1	53
LINE	LINE	Commitment to rights, but no policy recognition of threats. Score 1	Yes. Score 3	Inadequate notification within the app. Score 1	No, does not publish transparency report. Has taken public stance against encryption backdoors. Score 1	Provides specification of encryption, but not open source protocol. Score 1	47
VIBER MEDIA	VIBER	No commitment to freedom of expression, no policy recognition of threats. Score 1	Yes. Score 3	Inadequate notification within the app. Score 1	No, does not publish transparency report. Has publicly rejected encryption backdoors. Score 1	Provides specification of encryption, but not open source protocol. Score 1	47
KAKAO INC	KAKAO TALK	Commitment to rights, but no policy recognition of threats. Score 1	Has end-to-end encryption, but not set as a default. Score 1	Inadequate notification within the apps, no warning when using weaker encryption. Score 1	Publishes transparency report. Has taken public stance against encryption backdoors. Score 3	Only basic information on system of encryption. Score 0	40
MICROSOFT	SKYPE	Yes, clear commitment to rights and recognition of online threats. Score 3	Skype does not have end-to-end encryption. Score 0	No information or warnings within app about level of encryption on Skype. Score 0	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. Score 3	No specification of Skype system of encryption. Score 0	40
SNAPCHAT	SNAPCHAT	No commitment to freedom of expression, no policy recognition of threats. Score 1	Snapchat does not have end-to-end encryption. Score 0	No information given to users on website or in app about level of encryption. Score 0	Yes, and notifies affected user. Refuses to backdoor encryption. Score 3	No specification of Snapchat system of encryption. Score 0	26
BLACKBERRY	BLACKBERRY MESSENGER	No commitment to freedom of expression, no policy recognition of threats. Score 1	No, only offers end-to-end encryption as separate paid service. Score 0	Explanation on website, but no reference to encryption within app itself. Score 1	No, does not publish transparency report. Has publicly rejected encryption backdoors, but alleged cases where not done so in practice. Score 0	Provides specification of encryption, but not open source protocol. Score 1	20
TENCENT	QQ, WECHAT	No recognition of threats, no policy recognition of freedom of expression. Score 0	WeChat not end-to-end encrypted, QQ not end-to-end encrypted. Score 0	No information given to users on website or in app about level of encryption. Score 0	No, does not publish transparency report, does not publicly refuse to backdoor encryption. Score 0	No specification about encryption. Score 0	0

## WHICH COMPANY CAN READ YOUR PRIVATE MESSAGES?

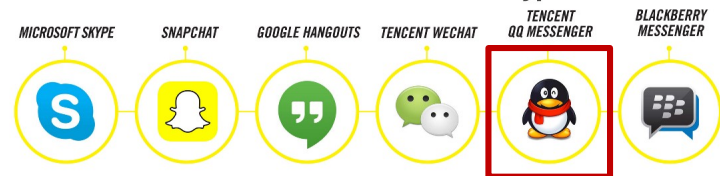
*Has end-to-end encryption as a default:*



*Has end-to-end encryption, but not set as default:*



*Does not have end-to-end encryption:*





## SUMMARY

### Summary

We should appreciate the astounding amount of free service available to us from Tencent. At the same time, the businesses that run these free services have a responsibility to their users.

Tencent's privacy policy has some pros and cons when it collects information, and how it uses and analyses the information. Thus, it includes the description of how user manage these data.



## REGISTER

### REASONABLE

- Provide customized and personalized needs
- Provide interest-based advertising
- Use for verifying user and identifying malware
  - i.e., Biological characteristic, password, etc.

### POTENTIAL RISK

- Violate the user's right to know
  - e.g., business planning, sell and share user personal information
- Provide interest-based advertising
- Decrease privacy
  - ***Biological characteristic*** is uniqueness

A mobile app registration screen with a blue header bar containing a back arrow and the text "Sign up". Below the header, there is a "Country" label with "China +86" selected. A text input field is labeled "Enter your phone num...". Below the input field is a blue button labeled "Next". At the bottom of the screen, there is a dark grey bar with the text "Do you accept Terms or Privacy?". Below this text are two buttons: a blue "Accept" button and a grey "Cancel" button.



## EVALUATION

# SOCIAL NETWORK

## REASONABLE

- Personalized advertising
  - based on **demographic** characteristics, location tracking and user information
- Useful for searching chat history

## UNCLEAR

- Intrude the right to know
  - e.g., Users cannot know how long their chat history will be kept & whether removed info still stored in database or not
- Intrude the right to forgotten
  - e.g., User is revealed by the images that other people post
- Data abuse
  - Sell user's data to the third parties **for commercial purposes**

Fuzhou University

Ad

Fuzhou University: Recruit adult freshmen from April 23.

CNY1980/yr then you can get bachelor degree after graduate.



Promotion ends in this WEEK!

Check

Tencent Advertisement

Ad

Do you want to join Tencent? Submit your resume now!



Still Available!

Join

58.com

Ad

House for rent: one bedroom and one bathroom. Only CNY300 /mo!



Still Available!

Check



## MINOR PROTECTION

### CLEAR VS. UNCLEAR

- the usage of service requiring the approval of their statutory guardian
- Information will be use for searching lost children
- Location tracking could invade the children's privacy
- At what age does informed consent is a basic principle for children?

#### Find people and things

Using your bluetooth and GPS information to help find losing children and things which wearing a QQ-IOT-chip.



QQWATCH



Peace of Mind . Peace of Heart

Easy to let go your hand but not your heart.

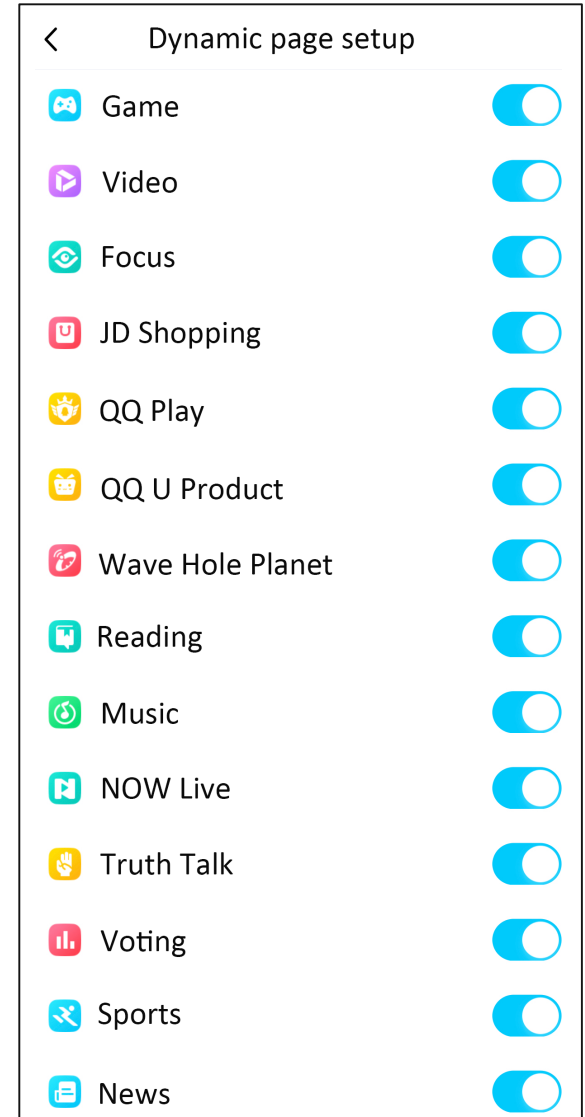
Tencent Children watch.

Let you feel relieved. Let the love follow.



## MISSING PRIVACY PROTECTIONS

- Do not have end-to-end encryption
  - i.e., surveillance, intercept.
- Do not promise the freedom of expression
- Do not disclose the government request for data
- Subscribe services to the user without permission
  - Pre-emptive opt-out





**Thank you for listening!**

2019.4.24

# Reference

- [1] Candeub, A. (2018, Oct 30). *Netflix's Race-Based Marketing Shows Potential For Anticompetitive Data Abuses*. Retrieved from <https://www.forbes.com/sites/washingtonbytes/2018/10/30/netflixs-race-based-marketing-shows-potential-for-anticompetitive-data-abuses/#11b22e3f3f48>
- [2] Zhao, A. (2019, April 24). *Chapter 2: Privacy*. Retrieved from [https://modules.lucbjtu.ac.uk/pluginfile.php/22705/mod\\_resource/content/1/2%20Privacy.pdf](https://modules.lucbjtu.ac.uk/pluginfile.php/22705/mod_resource/content/1/2%20Privacy.pdf)
- [3] Anon. (2019, April 24). *Privacy Statement of Netflix*. Retrieved from <https://help.netflix.com/legal/privacy>
- [4] Anon. (2019, Mar 11). *Privacy Issues with The Internet's Most Popular Websites*. Retrieved from <https://choosetoencrypt.com/news/privacy-issues-with-the-internets-most-popular-websites/>
- [5] Anon. (2019, April 24). *Tencent Privacy Protection Platform*. Retrieved from <https://privacy.qq.com/>