MESSAGE PRIVACY RANKING: HOW THE COMPANIES SCORED

Amnesty International ranked 11 technology companies on whether they are meeting their human rights responsibilities in the way they use encryption to protect users' online security. We focused specifically on instant messaging (IM) services. (See below for an explanation of the scoring system.)

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 encryption implementation criticised. **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 in Allo 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 commitment to freedom of expression. **Score 0**	WeChat not end-to-end encrypted, QQ encryption unclear. **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 publically refuse to backdoor encryption. **Score 0**	No specification about encryption. **Score 0**	**0**

We did not carry out an overall assessment of the security of the different messaging apps. Amnesty International recommends that journalists, activists, human right defenders and others whose communications may be particularly at risk seek expert digital security advice. We also did not rank the companies on their overall human rights performance, or their approach to privacy across all their products and services.

We ranked the companies across 5 criteria, awarding up to 3 points per criterion, based on whether our assessment determined that the company met the criteria completely (score 3), substantially but with room for improvement (score 2), only partially (score 1) or not at all (score 0). This gave a maximum possible score of 15, but for ease of understanding, we scaled the overall score as a total out of 100.