









Messenger	Telegram	Session
<div>Filter Table</div>		
Overview		
Is the app recommended to secure my messages and attachments?	No	Yes
Main reasons why the app isn't recommended	Bespoke cryptography	Implement perfect forward secrecy at the end-to-end encryption layer
/	Encryption not enabled by default	Provide more comprehensive independent assessments of security/privacy
Improvements to apps that are recommended	Data not protected, not all data protected	
Details		
Company jurisdiction	USA / UK / Belize / UAE	Switzerland
Infrastructure jurisdiction	UK, Singapore, USA, and Finland	Worldwide (uses de-centralised servers)
Implicated in giving customers' data to intelligence agencies?	No	No
Surveillance capability built into the app?	No	No
Does the company provide a transparency report?	No	Yes
Company's general stance on customers' privacy	Poor	Good
Company collects customers' data?	Poor	Good

<div>  Home Ratings Change Log About/FAQ Contact GitHub </div>		
Messenger	Telegram	Session
<div>Filter Table</div>		
Company collects customers' data?	Poor	Good
Funding	Pavel Durov	LAG Foundation Ltd
App collects customers' data?	Contact info / contacts / identifiers	No
User data and/or metadata sent to parent company and/or third parties?	Yes	No
Is encryption turned on by default?	No	Yes
Cryptographic primitives	RSA 2048 / AES 256 / SHA-256	X25519 / XSalsa20 256 / Poly1305
Are the app and server completely open source?	No (clients and API only)	Yes
Are reproducible builds used to verify apps against source code?	iOS and Android	No
Can you sign up to the app anonymously?	No	Yes
Can you add a contact without needing to trust a directory server?	No	Yes
Can you manually verify contacts' fingerprints?	No (session only, does not provide users' fingerprint information)	Yes
Directory service could	No	No

<div>  Home Ratings Change Log About/FAQ Contact GitHub </div>		
Messenger	Telegram	Session
<div>Filter Table</div>		
Can you manually verify contacts' fingerprints?	No (session only, does not provide users' fingerprint information)	Yes
Directory service could be modified to enable a MITM attack?	No	No
Do you get notified if a contact's fingerprint changes?	No (session only, does not provide users' fingerprint information)	N/A
Is personal information (mobile number, contact list, etc.) hashed?	No (session only, does not provide users' fingerprint information)	N/A
Does the app generate & keep a private key on the device itself?	Yes	Yes
Can messages be read by the company?	Yes	No
Does the app enforce perfect forward secrecy?	No (session keys do change after being used 100 times)	No
Does the app encrypt metadata?	No	Yes
Does the app use TLS/Noise to encrypt network traffic?	No	Yes
Does the app use certificate pinning?		Yes
Does the app encrypt data on the device? (iOS and Android only)		Yes



Messenger

Telegram

Session

Filter Table



Does the app encrypt metadata?

No

Yes

Does the app use TLS/Noise to encrypt network traffic?

No

Yes

Does the app use certificate pinning?

Yes

Does the app encrypt data on the device? (iOS and Android only)

Yes

Does the app allow local authentication when opening it?

Yes

Yes

Are messages encrypted when backed up to the cloud?

N/A, Session is excluded from iCloud/iTunes & Android backups

Does the company log timestamps/IP addresses?

Yes

No

Have there been a recent code audit and an independent security analysis?

Yes (November, 2015)

Yes (April, 2021)

Is the design well documented?

Somewhat

Somewhat

Does the app have self-destructing messages?

Yes

Yes