

Which Messaging Apps Offer the Most: Privacy, Anonymity, Security?

Secure Msging App	Privacy Level		Anonymity Potential		Cybersecurity Level		Adoption / Net Effect		Users (B)	Ease of Use	Customization	Best Use Case	PAC Score
<u>Session</u>	5	Decentralized, no phone number, no metadata logging	5	No phone number, fully anonymous	5	Decentralized, strong encryption	1		0.0	3	5	Fully anonymous , decentralized, no phone number, onion routing	15
<u>Matrix</u>	5	Decentralized, open-source, E2EE, no tracking	4	No phone number, public servers can expose metadata	5	Federated, open-source, audited, strong encryption	3		0.1	5	2	Decentralized, open-source msging for privacy-conscious users	14
<u>Signal</u>	5	Minimal metadata, no cloud backups, strong encryption	2	Requires phone num. VoIP, anon SIMs can work	5	Central, open-source, audited, strong encryption	3		0.1	4	4	Great privacy & security . But hard to get full anonymity	12
<u>iMessage</u>	4	Encrypted, but iCloud backups could expose messages	1	Requires Apple ID, strongly tied to real identity	3	Strong encryption, but closed-source	5		1.6	5	2	Apple users who trust Apple's ecosystem. Only Apple to Apple	8
<u>WhatsApp</u>	3	End-to-end encrypted, but Meta collects metadata	1	Phone number required, often linked to identity	3	Signal Protocol, but Meta controls infrastructure	5		2.0	5	2	Best for users who value flexibility , large groups over strong encryption	7
<u>Telegram</u>	2	Not encrypted by default, cloud-based, collects metadata	2	Phone number required, but usernames can reduce exposure	2	Encryption not default, proprietary cryptography	5		1.0	5	3	Users prioritizing convenience over security	6
Plain SMS	1	SMS msgs stored unencrypted, can be intercepted	1	Always linked to a phone number, easily tracked	1	No encrypt, SIM swap, intercept, metadata tracking	5		4.2	5	1	SMS is the worst in every category except ease of use, adoption	3

Privacy Level: How well does the app protect your messages and metadata from being accessed, tracked, or leaked? Evaluates encryption quality, metadata collection, telemetry, cloud backups, and third-party access. Higher scores mean less data collection and stronger protection against leaks.

Anonymity Potential: How difficult is it to link your use of the app to your real identity? Considers whether a phone number or other identifying information is required. Higher scores mean the app allows near-total anonymity.

Cybersecurity: How resilient is the app to exploits, hacking, and surveillance techniques? Looks at encryption strength, security audits, open-source transparency, and vulnerability to attacks. Higher scores mean the app has strong defenses against cyber threats.

Adoption & Network Effects: How easy is it to get others to use the app based on its user base and brand trust? Evaluates active user base, brand awareness, and friction in adoption. Higher scores mean the app is widely used and easy to convince others to install.

Ease of Use: How practical is the app for daily use without requiring technical knowledge or setup? Rates installation, interface usability, and general accessibility for non-technical users. Higher scores mean the app is simple to install and use.

Customization & Control: How much control does the user have over security settings, privacy options, and app behavior? Includes options for self-destructing messages, custom encryption settings, and security hardening. Higher scores mean greater user control over privacy.

