ObscureIQ's guide to

Messaging Services: Comparing Privacy, Anonymity, & Security

This comparison also looks at adoption & usability - because what good is a messaging tool if the people you need to speak with are not on it?

Tyoe	App	Open source	E2EE	Anonymity	Privacy Level		Anonymity Potential		Cybersecurity Level		PAC Score	Adoption / Net Effect	Users (M)	Ease of Use	Customization	Best Use Case	Recommendations
Decentralized Vanguard	**Briar**	Yes	Yes	High	5	P2P, Tor, no server	5	No ID required	5	Audited, Offline capable	15		1	2	5	Best when networks are censored or unreliable. Very low adoption.	Unreliable or censored networks
Decentralized Vanguard	**Session**	Yes	Yes	High	5	Decentralized, no phone, no metadata	5	No phone number, fully anonymous	4.5	Decentralized, strong encryption, but no battle-testing	14.5	1	1	3	5	Best for anonymity-first users who accept low adoption and friction.	High-risk environments where anonymity matters
Federated Ecosystem	**Matrix**	Yes	Yes	Mod	4.5	Decentral, E2EE, open-source, no track, admins trusted parties	4	No phone number, public servers can expose metadata	5	Federated, open-source, audited, strong encryption	13.5	3	115	5	2	Works well for technical teams and orgs that control their infrastructure.	Data sovereignty, self-hosted orgs
Federated Ecosystem	**Element**	Yes	Yes	Mod	4	E2EE, server dependent	4	No phone number	5	Audited, self-hostable	13		40	3	4	Tradeoff: complexity and trust in servers.	
Centralized Privacy	**Signal**	Yes	Yes	Low	5	Min metadata, no cloud bkup, strong encrypt	3	Phone req, unames dont cut telco/ social graph risk	5	Central, open-source, audited, strong encryption	13	3	70	4	4	Best for people who want secure messaging that others will actually use.	**Default for most people**
Centralized Privacy	**Threema**	Yes	Yes	High	5	Swiss servers, min metadata	3.5	No phone/email, app store/ ccnum trail	4	E2EE, audited	12.5	1	12	4	4	Best balance of anonymity, security, and day-to-day practicality.	**High privacy without phone numbers**
Hybrid and Niche	**Wire**	Part	Yes	Mod	4	E2EE, GDPR compliant	3	No phone req, but often uses email	5	E2EE, audited, open source	12	2	1	4	5	Best for businesses that need privacy without sacrificing structure.	Client onboarding for regulated environments
Hybrid and Niche	**Delta Chat**	Yes	Yes	Mod	4	rPGP, email metadata visible	3	Requires email address	4	Decentralized, audited	11		1	3	3	Security is solid, but privacy inherits email's weaknesses.	Low-risk client onboarding only
Corporate Giants	**iMessage**	No	Yes	Low	4	Encrypted, but iCloud backups could expose	1	Requires Apple ID, strongly tied to ID	3	Strong encrypt, closed-source	8	5	1,400	5	2	Best for users who trust Apple and comm only with other Apple users.	Apple-only reach and convenience
Corporate Giants	**WhatsApp**	No	Yes	Low	3	E2EE, extensive metadata collection for business model	1	Phone required, often linked to identity	3	Signal protocol, but Meta controls infrastructure	7	5	3,000	5	2	Best for users who value reach, large groups, adoption over privacy.	Cross-platform reach
Security Theater	**Telegram**	No	Part	Mod	2	Not encrypted by default, cloud-based, collects metadata	2	Phone req, unames cut exposure	2	Encryption not default, proprietary crypto	6	5	1,000	5	3	Best for broadcasts, communities, and convenience, not sensitive conversations.	Community and broadcast, not secure messaging
Security Theater	**Discord**	No	Part	Low	1	Data mining, no E2EE	2	Tracks IP/Hardware	2	Closed source, TLS only, gatekeepers	5		200	5	2	Best for gaming, creators, and public or semi-public groups.	Community coordination, not private messaging
Compromised	**Plain SMS**	No	No	Low	1	SMS msgs stored unencrypted, can be intercepted	1	Always linked to a phone, easily tracked	1	No encrypt, SIM swap, intercept, metadata tracking	3	5	4,000	5	1	Worst option for privacy, security, and metadata exposure.	Just don't.

- **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.
- PAC Score:: A weighted composite of Privacy, Anonymity, and Cybersecurity, not an endorsement.

- **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.