Security Comparison: TeleGuard vs. Olvid, Session, Telegram, Signal, and WhatsApp for Beginners

1. Executive Summary

This report compares the security and privacy of six popular messaging applications: TeleGuard, Olvid, Session, Telegram, Signal, and WhatsApp. The goal is to help beginner users, without in-depth technical knowledge, understand the key differences and choose the application that best suits their needs.

Teleguard, in short and simple

TeleGuard presents itself as a secure messaging application focused on privacy protection, developed by the Swiss company Swisscows AG. However, there are several significant concerns and reasons why one might consider avoiding TeleGuard:

1. **Lack of Transparency**: TeleGuard's source code is closed, meaning that independent experts cannot review or verify the security and privacy claims made by the application. This lack of transparency is a major drawback, as it requires users to blindly trust the developers without any verifiable evidence.

2. **No Independent Security Audits**: There are no known independent security audits for TeleGuard. Security audits are crucial as they provide an external review of the application's security measures, helping to identify vulnerabilities and ensure that the application is secure.

3. **Use of Non-Standard Encryption Protocol**: TeleGuard uses the SALSA20 encryption algorithm, which, while respected in certain contexts, is not a standard protocol for end-to-end encryption in messaging applications. The implementation details for how SALSA20 is used to ensure end-to-end encryption are not provided, making it difficult to assess the robustness of the encryption.

4. **Contradictory Claims**: TeleGuard claims to offer total anonymity and not to collect any user data, including IP addresses. However, there are user reports of unexpected behavior, such as the reappearance of deleted discussions after reinstallation, which suggests some form of data storage or linking on the server side.

5. **Questionable Practices**: The requirement to purchase a custom ID raises questions about data collection and potential associations with user accounts, despite denials from the company. This practice could undermine the privacy and anonymity promises.

6. **Lack of Verifiable Evidence**: The strong claims of security and privacy made by TeleGuard are not backed by verifiable evidence. This makes it difficult for users to trust the application fully.

7. **Potential Risks of "Homegrown" Implementation**: The use of a less common and non-standard encryption protocol that hasn't been widely validated by the security community introduces potential risks, especially if the implementation is not thoroughly vetted.

In summary, while TeleGuard makes appealing claims about security and privacy, the lack of transparency, independent audits, and verifiable evidence, combined with the use of non-standard protocols and questionable practices, make it a risky choice for users concerned about their privacy and security.

Key Findings

- **Signal** and **Olvid** are often considered the most secure overall. **Signal** offers robust end-to-end encryption (E2EE) by default for all communications, collects very little data (metadata), is fully open-source, and is funded by a non-profit foundation, which inspires confidence[1]. **Olvid** goes further by also encrypting metadata (who talks to whom) and uses a unique architecture that does not rely on trust in servers, validated by French certifications (ANSSI) and experts[2]. Olvid does not require any personal identifiers[3].
- **Session** stands out for its very high level of anonymity, requiring neither a phone number nor an email, and for its advanced protection of metadata through a decentralized network (similar to Tor)[4]. However, this architecture can sometimes affect speed, and some features are less mature[4].
- **WhatsApp**, while using the same E2EE encryption protocol as Signal by default for personal conversations[5], is owned by Meta (Facebook). This raises major concerns as the app collects a significant amount of metadata that is shared with Meta, whose business model relies on the exploitation of user data[5]. Additionally, message backups in the cloud are not encrypted by default[6].
- **Telegram** is very popular and offers many features, but its default security is weak: E2EE is not enabled for normal discussions and is impossible for groups[7]. You must manually use "Secret Chats" for E2EE protection (limited to two-person conversations). Its in-house encryption protocol (MTProto) and metadata collection have been criticized by experts[8].
- **TeleGuard** promises high anonymity (no phone number required, use of a unique ID) and servers based in Switzerland[9]. However, the app severely lacks transparency: its source code is closed, and no independent security audit has been published[10]. It is therefore impossible to verify its security claims, which represents a significant risk. Its encryption protocol (SALSA20) is less common for this type of use[10].

General Recommendation for Beginners

For a user seeking a good balance between verifiable strong security, ease of use, and a large user base, **Signal** is often the most recommended choice[11]. For those whose absolute priority is maximum confidentiality and anonymity, even at the cost of some compromises on speed or ease,

Session or **Olvid** are very solid options[6]. **WhatsApp** remains practical due to its popularity but involves accepting significant monitoring of your habits by Meta[5]. **Telegram** requires very careful use (systematic activation of "Secret Chats" for sensitive conversations) and has structural weaknesses[12]. **TeleGuard** does not provide enough evidence of its security to be confidently recommended[10].

2. Introduction: Why Messaging Security is Important

Our daily conversations are increasingly taking place through messaging applications on our smartphones. Whether it's exchanging news with loved ones, discussing professional projects, or sharing personal information, we entrust a lot of data to these tools. But are they really private?

Online conversations can be vulnerable. Without adequate security measures, your messages could be intercepted by hackers, read by the company providing the application, or exposed during a data leak. It is therefore essential to choose an application that effectively protects your exchanges.

Protection is not only about the content of your messages (what you write). It also concerns metadata: information about your messages. For example: who is talking to whom, at what time, from what approximate location (via your IP address), and how often. This metadata can reveal a lot about your habits, relationships, and private life, even if the exact content of the messages remains secret.

This report aims to inform you about the security of six messaging applications: TeleGuard, Olvid, Session, Telegram, Signal, and WhatsApp. We will compare them based on several key criteria, explained simply, to help you make an informed choice.

Simplified Key Terms

- **End-to-End Encryption (E2EE)**: Like sending a letter in a locked box. Only you and your recipient have the unique key to open it. No one else—not even the postal service (the company behind the app)—can read the contents of the letter during transport. This is the best protection for the content of your messages.
- **Metadata**: Information visible on the envelope of your letter: the name and address of the sender and recipient, the date sent, the postmark. They do not reveal the content of the letter but provide a lot of information about the exchange itself. Some apps protect the content but collect a lot of metadata.
- **Open Source**: Imagine that the construction plans for the locked box and the postal service are public. Anyone, especially security experts, can verify how the app is built, ensure it is solid, and that there are no hidden "backdoors." This is a significant guarantee of transparency and trust.
- **Centralized vs. Decentralized Servers**:
  - **Centralized**: All messages (or information about messages) go through a main data center controlled by the company (like a central post office). This is simpler to manage but

creates a single point of control and vulnerability.
    - **Decentralized**: Messages transit through a network of several independent servers (or "nodes"), often managed by the community (like a network of local post offices). This makes surveillance and censorship more difficult as there is no central point.
- **Independent Security Audit**: This is like subjecting the app to a thorough technical inspection by a specialized cybersecurity firm. These experts actively seek out flaws and weaknesses. Publishing these audits strengthens confidence in the app's security.

3. Detailed Analysis by Application

Let's now examine each application in more detail, focusing on their security, privacy, and the organization behind them.

3.1 TeleGuard

TeleGuard presents itself as a secure messenger focused on privacy protection, developed by the Swiss company Swisscows AG[9].

- **Security**:
    - **Encryption**: TeleGuard claims to use end-to-end encryption (E2EE) for all text, voice messages, as well as voice and video calls. The mentioned algorithm is SALSA20, described as "one of the best encryption algorithms currently available"[9]. The connection to the servers uses HTTPS[9]. SALSA20 is a stream cipher designed by Daniel J. Bernstein, known for its speed[13]. Although the algorithm itself is respected (the full version Salsa20/20 resists known attacks well[14]), its use for E2EE in messaging is less standard than other protocols like the Signal Protocol. Additionally, TeleGuard provides no technical details on how SALSA20 is implemented to ensure E2EE (key management, authentication, forward secrecy, etc.)[10]. This lack of information makes it difficult to assess the actual robustness of the encryption.
    - **Metadata Collection**: The application claims not to collect any user data, including IP addresses, and not to record the browsers or operating systems used[9]. Messages are allegedly deleted from servers immediately after delivery[9]. These claims are very strong but are undermined by the lack of verifiable evidence. Users have reported contradictory experiences, such as the reappearance of deleted discussions after reinstallation or the reassignment of the same ID, suggesting some form of server-side storage or data linking[15]. The privacy policy mentions the collection of email and payment information for actions on the website (such as purchasing a custom ID[9]), but states that this data is not linked to activity within the app[16].
    - **Identifier and Anonymity**: TeleGuard does not require a phone number or email address to use the app[9]. Each user receives a unique "TeleGuard ID" (a 9-digit number and a QR code) that serves as an identifier to add contacts[9]. It is possible to purchase a custom ID[9]. The app claims total anonymity[9]. Not linking the app to a phone number is an

advantage for anonymity[17]. However, the TeleGuard ID remains a unique and persistent identifier linked to the user[17]. Purchasing a custom ID raises questions about the collection of payment data and their potential association with the account, despite the company's denials[18].

- **Server Architecture**: The servers are centralized and located in data centers in Switzerland[9]. TeleGuard claims that this location exempts them from EU/USA data protection laws while complying with the GDPR (General Data Protection Regulation)[9]. The location in Switzerland is often seen as positive for privacy[19]. However, the centralized architecture implies full trust in the operator (Swisscows AG). The claim of GDPR compliance while not being subject to EU laws seems contradictory[9].
- **Source Code and Audits**: The source code of TeleGuard is not public (closed source)[10]. No independent security audit conducted by an external company has been published or even mentioned[10]. This is a major drawback. Without access to the code and without audits, it is impossible to independently verify TeleGuard's security and privacy claims. Users must rely entirely on the developer's statements.

- **Structure and Economic Model**:
  - **Organization**: TeleGuard is a product of Swisscows AG, a Swiss anonymous company[9]. Swisscows AG itself is owned by Hulbee AG, also Swiss and led by Andreas Wiebe[19]. Swisscows also operates a search engine that claims to be privacy-friendly[9].
  - **Funding and Governance**: Funding comes from donations to Swisscows, potential sales of custom TeleGuard IDs, and a future professional version of TeleGuard[9]. The model is based on the overall Swisscows ecosystem[9]. Funding through donations and premium services is generally better aligned with privacy than an advertising model. However, the private company structure implies commercial objectives.

Evaluation of TeleGuard's Claims

TeleGuard builds its image on very strong promises of anonymity and security: no phone number, no metadata collection, servers in Switzerland, solid encryption[9]. These promises are appealing. However, the complete lack of transparency—closed source code, no published security audits—creates a fundamental contradiction[10]. Users are invited to blindly trust Swisscows AG without any verifiable evidence. This is a risky bet in the field of security, especially when compared to open-source and audited alternatives. User testimonies reporting unexpected behavior of the app[15] only reinforce this skepticism.

Additionally, the choice of the SALSA20 algorithm[9] is unusual for modern E2EE messaging. Industry leaders prefer comprehensive and proven protocols like the Signal Protocol or libraries like libsodium. Although SALSA20 is a respected stream cipher[13], its correct implementation for E2EE (which goes far beyond simple encryption) is complex and not documented by TeleGuard[10]. One might wonder if this technical choice is justified or if it reflects a lack of alignment with recognized best practices, introducing a potential risk associated with an unvalidated "homegrown" implementation.

3.2 Olvid

Olvid is a messaging application developed in France, which highlights a unique security model and strong cryptographic guarantees[2].

- **Security**:
  - **Encryption**: Olvid uses E2EE by default for all exchanges: messages, attachments (regardless of size), audio and video calls (individual and group in the premium version)[2]. Each message and file uses a different and single-use encryption key, ensuring persistent confidentiality (Forward Secrecy)[2]. Uniquely, Olvid also encrypts metadata, preventing even Olvid servers from knowing "who is talking to whom"[2]. Olvid uses its own cryptographic protocols, designed by its founder cryptographers and scientifically validated by external researchers (Michel Abdalla, CNRS, IACR)[2]. The application is also preparing for the post-quantum era[2]. Metadata encryption is a major advantage in terms of confidentiality compared to almost all other messaging apps.
  - **Metadata Collection**: Olvid claims not to collect any personal data and not to leave any traces on its servers. Thanks to metadata encryption and its architecture, the server technically cannot know who is communicating with whom[2].
  - **Identifier and Anonymity**: The application does not require a phone number or email address to function[3]. The identity of contacts is established and verified directly between users, either by scanning a QR code or via a secure corporate directory in the paid version[3]. There is no central user directory[6]. This offers a very high level of anonymity. Adding contacts is more manual than on other applications, which can be seen as less convenient but strengthens security by avoiding risks associated with automatic address book synchronization.
  - **Server Architecture**: Olvid uses a revolutionary architecture that does not rely on trust in servers ("No trust in servers")[2]. Servers act as simple relays for encrypted messages, never being able to access either the content or the metadata. Even in the event of a hack of Olvid servers, communications would remain confidential and identities protected, as security relies entirely on client-side cryptography[2]. External sources mention the use of cloud infrastructures such as Amazon Web Services[20], but Olvid's security model is designed to make this location irrelevant for data confidentiality. This model is theoretically superior to traditional centralized and even decentralized architectures.
  - **Source Code and Audits**: Olvid client applications (iOS, Android) are open-source, published under the AGPLv3 license[2]. The server-side code remains proprietary[20]. Olvid is the only messaging app to date to have received two First-Level Security Certifications (CSPN) issued by the French National Agency for the Security of Information Systems (ANSSI), for its iOS and Android versions[2]. The protocols have been scientifically validated[2], and the company participates in a public bug bounty program[20]. This combination (open-source client, high-level government certifications, scientific validation, bug bounty) offers an exceptional level of transparency and assurance.

- **Structure and Economic Model**:
    - **Organization**: Olvid is developed by Olvid SAS, a private French company based in Paris, founded in 2017/2019 by cryptography experts[20].
    - **Funding and Governance**: Olvid uses a freemium economic model. Essential features (E2EE text messaging, attachments, groups, receiving secure calls) are free. Advanced features, mainly aimed at professionals and businesses (initiating group audio/video calls, using Olvid on multiple devices simultaneously, administration console for centralized deployment and management), are paid through Olvid Enterprise[3]. Olvid has also received funding from investors, including BNP Paribas and Wavestone[21]. This freemium model, focused on added value for paying customers, is structurally aligned with confidentiality promises. There is no incentive to exploit the data of free users to generate revenue, unlike advertising-based models.

Evaluation of Olvid

Olvid positions itself as offering the strongest and most proven security guarantees on the current market, thanks in particular to metadata encryption, its trustless server model, and its credible external validations (ANSSI, scientific research, open-source client code)[2]. This emphasis on mathematically demonstrable security is its main asset. However, this excellence has potential trade-offs: a smaller user base than giants like WhatsApp or Telegram, which can limit its usefulness if your contacts do not use it (network effect), and a contact addition process that requires a voluntary action (QR code exchange), less immediate than automatic address book synchronization[6]. Choosing Olvid thus represents a clear trade-off: maximum and verifiable security and confidentiality, in exchange for potentially lower popularity and convenience.

Its freemium economic model[3] enhances its credibility in terms of privacy. By deriving its revenue from professional licenses and advanced features, Olvid does not need to monetize the data of its free users. This economic model is therefore in perfect alignment with its stated mission of absolute confidentiality protection, distinguishing it from platforms whose revenue intrinsically depends on the collection of user data[5].

3.3 Session

Session is a messaging application focused on anonymity and metadata protection, using a decentralized network[4].

- **Security**:
    - **Encryption**: Session uses E2EE by default for individual and group messages[4]. It is based on the "Session Protocol," which itself is built on the recognized cryptographic library libsodium[4]. Voice and video calls are also E2EE encrypted, but they use a direct connection between users (peer-to-peer, P2P). This P2P mode, unlike messages, does not go through the anonymization network and can therefore reveal the IP addresses of the participants to each other[4]. This is an important compromise to be aware of for calls.

- **Metadata Collection**: The design of Session aims to radically minimize the collection of metadata. The application does not require a phone number, email, location data, or device information[4]. Its main advantage is the use of a decentralized network of servers ("Service Nodes") and an **onion routing** system, similar to that of Tor[4]. This system routes messages through multiple intermediate nodes, so that no single node knows both the sender and the recipient. This allows the user's IP address to be masked and protects the "social graph" (who communicates with whom)[4]. This is superior metadata protection compared to centralized messaging services.
- **Identifier and Anonymity**: Session offers a very high level of anonymity. No phone number or email is required to create an account[4]. The identifier is a "Session ID," a long randomly generated string of characters[22]. Users choose a display name that can be a pseudonym[4]. To back up and restore an account (for example, when changing phones), the user must imperatively keep a **recovery phrase** secret[4]. The security of the account relies entirely on the user's proper management of this phrase.
- **Server Architecture**: Session uses a **decentralized** architecture. Messages are relayed by a network of "Service Nodes" operated by a global community of operators[4]. This network uses onion routing to protect privacy[4]. Messages that cannot be delivered immediately are temporarily stored (for a maximum of 14 days) by a group of nodes ("swarm") before being deleted[4]. Attachments are encrypted and stored on a dedicated file server (Oxen File Server), but access to this server is also protected by onion routing to mask the IP[4]. This decentralization enhances resistance to censorship and avoids a single point of failure[23]. However, it can sometimes result in some latency in message delivery, especially if the "slow mode" option is used[4].
- **Source Code and Audits**: Session applications (for desktop, Android, and iOS) are fully **open-source**[4]. The node network is based on the Oxen project, which is also open-source. Session underwent a security audit by the specialized firm Quarkslab in 2021. The audit revealed no critical vulnerabilities, only a few minor issues that were fixed[4]. Open-source and this audit enhance trust, although a more recent audit would be welcome.

- **Structure and Economic Model**:
  - **Organization**: Session was initially managed by the Oxen Privacy Tech Foundation (OPTF), an Australian foundation[24]. At the end of 2023/beginning of 2024, facing a regulatory environment deemed less favorable in Australia, management was transferred to the **Session Technology Foundation** (Session Technology Stiftung), a non-profit foundation based in **Switzerland**[4]. This choice of Switzerland aims to benefit from a more protective legal framework for privacy and encryption[25].
  - **Funding and Governance**: The operation of Session's decentralized network relies on economic incentives linked to a cryptocurrency. Operators of Service Nodes must "stake" a certain amount of the **$SESH** (Session Token) to participate in the network and are rewarded in $SESH for their contribution[4]. This mechanism aims to ensure the robustness and decentralization of the network. The development of the application itself is supported by the foundation and potentially by future premium features that could be

purchased in $SESH or traditional currency[26]. This cryptocurrency-based model is unique among the applications compared here.

Evaluation of Session

Session stands out for its radical commitment to anonymity and metadata protection, thanks to the absence of personal identifiers at registration and its decentralized architecture using onion routing[4]. This is its major comparative advantage. However, this approach involves compromises. Decentralization and onion routing can sometimes reduce the speed of message delivery compared to centralized systems[11]. Voice/video calls, while E2EE encrypted, do not benefit from network anonymization and expose IP addresses between participants[4]. Total anonymity places the crucial responsibility of managing the recovery phrase on the user[4]. Finally, the funding model based on a cryptocurrency ($SESH) is innovative but may seem complex or volatile to some users[26].

The recent transfer of Session's management to a foundation based in Switzerland[25] is a strong and positive signal. It aligns the app's legal structure with its privacy protection mission, choosing a jurisdiction known for its favorable laws[25]. This enhances Session's credibility and its potential resistance to data access requests, differentiating it from apps based in countries with more extensive surveillance laws. Session therefore represents a solid choice for those who prioritize anonymity and metadata protection above all else and are willing to accept the associated compromises in terms of performance or management.

3.4 Telegram

Telegram is an extremely popular messaging application known for its speed, interface, and numerous features, particularly large groups and broadcast channels[11].

- **Security**:
    - **Encryption**: This is the most controversial point about Telegram. By default, normal discussions ("Cloud Chats") are **NOT end-to-end encrypted (E2EE)**[7]. They use encryption between the client and the server, and then between the server and the client. This means that **Telegram has access to the encryption keys and can read the content of these messages** on its servers[7]. To benefit from E2EE, you must **manually activate** the **"Secret Chat"** option for each individual conversation[7]. This option is **not available for group discussions**[7]. Voice and video calls, however, seem to be E2EE by default[27]. Telegram uses its own encryption protocol, **MTProto**, developed in-house[28]. This protocol has been criticized by many cryptography experts for being "homegrown," its initial lack of public audits, and certain weaknesses or design choices deemed risky, although improvements have been made (MTProto 2.0) and some recent analyses are more nuanced[8]. The lack of E2EE by default for the majority of exchanges is a major disadvantage compared to other applications in this comparison.
    - **Metadata Collection**: Telegram collects a certain amount of metadata, including the **phone number** used for registration, user **contacts** (if permission is given to sync them),

the **IP address**, information about the **devices** used, and the history of username changes[7]. This data can be kept for up to 12 months[29]. Telegram claims not to use this data for targeted advertising purposes[29], but it is nevertheless collected and stored and could be accessible to Telegram or disclosed upon legal request[30].

- **Identifier and Anonymity**: A **valid phone number is required** to create a Telegram account[31]. This number is the main identifier linked to the account. It can be hidden in privacy settings so that it is not visible to users who are not in your contacts[7]. You can also set a public username (@username) that allows you to be contacted without sharing your number. Anonymity is therefore limited by the need to provide a phone number.
- **Server Architecture**: Telegram uses a **centralized** architecture, with servers distributed in various data centers around the world for performance and availability reasons[29]. The encryption keys for "Cloud Chats" (non-E2EE) are also stored by Telegram, albeit in a distributed manner for internal security reasons[29]. This centralization, combined with weak default encryption, gives Telegram considerable control and access to user data.
- **Source Code and Audits**: Telegram's client applications (mobile, desktop, web) are **open-source**, allowing for some transparency[11]. However, the **server-side code is not open-source**[27]. Regarding the MTProto protocol, although academic analyses have been conducted[32], Telegram does not regularly publish formal and independent security audits of its entire system, unlike Signal, for example[27]. Criticisms of the MTProto design persist[8].

- **Structure and Economic Model**:
  - **Organization**: Telegram was founded by Russian brothers Pavel and Nikolai Durov[33]. Pavel Durov is the CEO and public figure[34]. The company (often registered under names like Telegram Messenger LLP) is generally considered to be based in Dubai, although its exact legal structure remains opaque[7]. Pavel Durov left Russia after conflicts with authorities over his previous social network, VKontakte[33].
  - **Funding and Governance**: Historically, Telegram has been funded by Pavel Durov's personal fortune[34]. A major attempt at fundraising through a cryptocurrency offering (ICO for the TON/Gram project) failed due to regulatory issues, particularly with US authorities[34]. Since then, Telegram has turned to monetization through a **Telegram Premium** subscription offering additional features, and a discreet advertising platform broadcast only in large public channels (Telegram claims that these ads are based on the channel's topic and not on users' personal data)[29]. This model is potentially less intrusive than traditional targeted advertising but introduces a commercial logic. The opacity of the company's structure and its base in Dubai make governance difficult to evaluate.

Evaluation of Telegram

Telegram illustrates a paradox: it is extremely popular and often perceived as a "secure messaging" app, especially by those looking for an alternative to WhatsApp[8]. However, this reputation is largely overstated or based on a misunderstanding of its actual operation[12]. The technical reality is that Telegram's default security is weak because it does not use E2EE for most conversations

(Cloud Chats and all groups)[7]. The user must actively choose "Secret Chats" (limited to two-person discussions) to obtain E2EE protection[7]. Additionally, its in-house MTProto protocol, although improved, has been criticized and does not enjoy the same level of trust as standards like the Signal Protocol[8]. Finally, Telegram collects non-negligible metadata[29]. Its popularity thus seems more due to its fast interface, rich features (unlimited large groups, channels, bots, large file sharing), and "rebel" image than intrinsically superior security compared to competitors like Signal or Olvid.

The choice to develop and maintain its own cryptographic protocol, MTProto, rather than adopting proven standards, remains a fundamental point of debate and perceived risk[8]. Even if MTProto 2.0 is considered more robust[30], the protocol's history, past flaws (even theoretical ones), and the lack of regular and comprehensive third-party audits[27] maintain uncertainty. For a novice user, this raises the question of trust: should one rely on a less proven "homegrown" protocol or prefer solutions based on standards widely validated by the international community of security experts? Using Telegram for sensitive communications without systematically activating "Secret Chats" amounts to trusting Telegram not to access your messages.

3.5 Signal

Signal is a widely recognized messaging application for its strong commitment to security and privacy, developed by a non-profit foundation[1].

- **Security**:
    - **Encryption**: Signal uses **E2EE by default for absolutely all communications**: individual messages, group messages, audio calls, video calls, attachments, and even stickers[1]. It uses the **Signal Protocol**, an open-source encryption protocol considered the gold standard in messaging security[1]. This protocol is so respected that it has been adopted and implemented by other major players like WhatsApp, Google (for RCS messages), and Skype[35]. The robustness and reliability of Signal's encryption are widely recognized by experts.
    - **Metadata Collection**: Signal is designed from the ground up to **collect the absolute minimum of metadata** necessary for its operation[1]. The app does not store information about your contacts, the groups you belong to, your profile, or who you communicate with. The only information Signal admits to keeping on its servers is technical: essentially, the registered phone number (stored as a cryptographic hash), the account creation date, and the date of the last connection to the service[36]. Signal has even proven during legal requests (subpoenas) that it could provide almost no useful data about its users[37]. Advanced techniques like "Sealed Sender" are used to attempt to mask the sender of a message even from Signal's servers.
    - **Identifier and Anonymity**: Historically, Signal required a **phone number** for registration, which was its main weakness in terms of anonymity[36]. However, Signal has recently introduced major features to address this criticism: the ability to create and use **usernames** to be contacted, and the **"Phone Number Privacy"** feature that allows you to

hide your phone number from your contacts and Signal itself as much as possible[37]. Although a phone number is still required for initial registration (to prevent spam), it is no longer necessary to share it to communicate. This significantly improves the potential for anonymity on Signal.

- **Server Architecture**: Signal uses a **centralized** architecture, managed by the Signal Foundation[38]. However, the servers are designed to be "ignorant" relays: thanks to E2EE and extreme minimization of metadata, they do not have access to the content of communications or most contextual information[36]. The main risk associated with centralization is therefore a potential service interruption rather than a breach of confidentiality via the servers.
- **Source Code and Audits**: Signal is a model of transparency: **all of its code, both for client applications (iOS, Android, Desktop) and server code, is open-source** and publicly available for review[1]. Additionally, the Signal protocol and applications have undergone **multiple independent security audits** over the years, conducted by recognized cybersecurity firms[27]. The results of these audits are often publicly discussed. This maximum transparency and repeated external validations inspire great confidence.

- **Structure and Economic Model**:
  - **Organization**: Signal is developed by Signal Messenger LLC, an entity wholly owned by the **Signal Technology Foundation**, a **non-profit foundation** registered under 501(c)(3) status[1]. It was co-founded by Moxie Marlinspike (the cryptographer behind Signal) and Brian Acton (co-founder of WhatsApp, who left Facebook/Meta due to disagreements over privacy)[35]. The current president is Meredith Whittaker, a recognized advocate for privacy[35].
  - **Funding and Governance**: Signal is funded **exclusively by donations** from its users and grants[1]. Brian Acton provided a substantial initial donation of $50 million to launch the foundation[35]. There is **no advertising, no external investors seeking financial returns, and no sale of user data**[1]. The non-profit structure ensures that the mission of privacy and security protection takes precedence over any profit considerations. The foundation publishes its financial statements (Form 990 in the United States), offering transparency regarding its revenues and expenses[37]. This model is considered the most aligned with privacy objectives.

Evaluation of Signal

Signal has firmly established itself as the reference in secure E2EE messaging. Its main strength lies in the combination of encryption technology (the Signal Protocol) recognized as the gold standard, open-source, and widely audited, with an application that applies this encryption by default to all exchanges[1]. The fact that this protocol has been adopted by major players like WhatsApp and Google is a testament to its robustness[35]. Signal's complete transparency (open-source client and server code, regular audits[37]) and its non-profit funding structure through a foundation dedicated to privacy[38] significantly enhance trust. Signal does not just promise security; it provides the evidence and mechanisms to verify it.

The historical criticism regarding the requirement to use a phone number, which limited anonymity, has been largely addressed by the recent introduction of usernames and the "Phone Number Privacy" feature[37]. This major development shows that Signal listens to its community and actively seeks to improve privacy protection beyond content encryption. Signal is increasingly successful in offering a balance between very high-level security, strong metadata confidentiality, exemplary transparency, and ease of use that allows it to reach a wide audience, not just security experts[11].

3.6 WhatsApp

WhatsApp is the most widely used messaging application in the world, owned by Meta (formerly Facebook)[11].

- **Security**:
    - **Encryption**: WhatsApp uses **E2EE by default** for most communications between individual users: text and voice messages, audio and video calls, photos, videos, documents, status updates, and live location sharing[5]. The application uses an implementation of the **Signal Protocol**, the same robust protocol as Signal[5]. However, there are important exceptions: messages exchanged with **business accounts** may not be E2EE[11]. More critically, **backups of chat history to the cloud (Google Drive for Android, iCloud for iOS) are NOT E2EE encrypted by default**[6]. Although there is an option to enable E2EE encryption for backups, it must be **manually activated** by the user and requires the creation of a password or a specific key[39]. Without this manual activation, the entire message history, although encrypted during transmission, becomes accessible in plaintext to Google/Apple or anyone accessing these cloud accounts.
    - **Metadata Collection**: This is the **major weak point** of WhatsApp in terms of privacy. The application **collects a very large amount of metadata**[5]. This includes: your phone number, the phone numbers of your contacts (if you allow access to the address book), your profile name and photo, information about your usage (when you use the app, which features, who you interact with most frequently), technical information about your device and connection (model, OS, battery level, signal strength, **IP address**), your approximate location (deduced from the IP) or precise location (if you share your location), information about transactions if you use payment functions, and data about your interactions with business accounts[5]. This metadata is **shared with the parent company, Meta (Facebook)**, and used for various purposes, including improving Meta services, security, and potentially for targeted advertising on other Meta platforms (Facebook, Instagram)[5].
    - **Identifier and Anonymity**: Using WhatsApp **mandatorily requires a valid phone number** for registration and operation[5]. This number is the user's primary identifier and is generally visible to their contacts. There is **no possibility of anonymity** either towards WhatsApp/Meta or towards your contacts.
    - **Server Architecture**: WhatsApp uses a **centralized** architecture, managed by Meta[5]. The servers act as relays for E2EE encrypted messages (they cannot read the content), but they actively collect, store, and process the large amount of metadata mentioned

above[5]. Centralization at Meta is a cause for concern due to the company's business model[40].

- **Source Code and Audits**: The source code of the WhatsApp application is **closed-source**[41]. Although the underlying encryption protocol (Signal Protocol) is open-source, WhatsApp's specific implementation is not public, preventing a complete independent verification[41]. Meta likely conducts internal security audits but does not publish them transparently as Signal or Olvid do.

- **Structure and Economic Model**:
  - **Organization**: WhatsApp Inc. is a **subsidiary of Meta Platforms, Inc.**, one of the world's largest technology giants[5]. Facebook acquired WhatsApp in 2014 for the colossal sum of $19 billion[40].
  - **Funding and Governance**: The WhatsApp application is free for end users. Its value to Meta lies in its integration into the company's global ecosystem. The metadata collected by WhatsApp is used to **improve other Meta products** (such as Facebook and Instagram) and to **refine targeted advertising** on these other platforms[5]. Meta also develops **paid services for businesses** through the WhatsApp Business API, allowing them to communicate with their customers via WhatsApp[39]. It is important to note that the original founders of WhatsApp, Jan Koum and Brian Acton, both left Meta/Facebook after the acquisition, citing deep disagreements over the monetization strategy and the weakening of user privacy protection[35].

Evaluation of WhatsApp

WhatsApp embodies the most widespread compromise for billions of users worldwide. On one hand, it offers good security for the content of personal messages, thanks to the use of the robust Signal Protocol for default E2EE[5]. On the other hand, it offers unmatched ease of use and popularity: it is very likely that most of your contacts already use WhatsApp, making it extremely practical[11]. However, this convenience and apparent security come at a high cost in terms of metadata privacy. By using WhatsApp, you accept that Meta (Facebook) collects a massive amount of information about your communication habits (who, when, where, how) and uses it for its own commercial purposes[5]. For a novice user, the choice is therefore clear: prioritize ease of connection with your existing network or refuse surveillance of your metadata by one of the world's largest data collectors.

A crucial technical point, often overlooked, concerns **cloud backups**. By default, they are not E2EE encrypted[6]. This means that if you use the backup function (very practical for not losing your messages when changing phones), your entire conversation history, although protected during the initial exchange, becomes vulnerable once stored on Google or Apple servers. Manually activating the **E2EE encrypted backup** option[39] is an **absolutely essential** step to maintain any semblance of long-term confidentiality with WhatsApp. Without this action, the protection offered by E2EE is largely nullified from the first backup.

4. Systematic Comparison

After examining each application individually, let's compare them directly on key aspects of security and their structure.

4.1 Comparative Table: Security Features

The following table summarizes the technical security characteristics of each application.

Feature	TeleGuard	Olvid	Session	Telegram	
E2EE by Default	Claimed Yes[9]	Yes[2]	Yes (Messages)[4]	No (Cloud Chats) / Yes (Secret Chats)[7]	Yes[1]
Encryption Protocol	SALSA20 (Proprietary/Non-standard)[9]	Custom Protocols (Validated)[2]	Session Protocol (Libsodium)[4]	MTProto (Proprietary, Criticized)[28]	Signa (Gold
Metadata Encryption	No	Yes[2]	Partial (Onion Routing)[4]	No[29]	Partia Techr
Key Metadata Collection	Claimed None (IP, etc.)[16]	None (No personal data)[3]	Very Low (No Phone/Email/IP msg)[22]	Yes (Phone, IP, Contacts, Usage)[29]	Very Phon
Required Identifier	TeleGuard ID[9]	None (Direct Verification)[3]	Session ID[22]	Phone Number[29]	Phon (but mask[36]
Possible Anonymity Level	High (Claimed)	Very High	Very High	Low/Medium	Medi usern
Server Architecture	Centralized[9]	Trustless (Relay)[2]	Decentralized (Service Nodes)[4]	Centralized[29]	Centr (Mini

Feature	TeleGuard	Olvid	Session	Telegram	
Server Location	Switzerland[9]	Not Relevant (Crypto Model)	Global (Community)	Global (Distributed)[29]	USA (
Client Source Code	Closed[10]	Open (AGPLv3)[42]	Open[23]	Open[11]	Open
Server Source Code	Closed	Closed[20]	Open (Oxen)	Closed[27]	Open
Independent Security Audits	None Known[10]	Yes (ANSSI, Scientific, Bug Bounty)[2]	Yes (Quarkslab 2021)[4]	Limited / Irregular[8]	Yes (I Regu
Certifications	None Known	ANSSI CSPN (iOS,	None Known	None Known	None

This table highlights the fundamental technical differences. Olvid and Session stand out for their approach to anonymity and metadata. Signal excels with its standardized protocol, transparency, and default E2EE. WhatsApp shares Signal's good protocol but fails on metadata and transparency. Telegram lags on default E2EE and its protocol. TeleGuard makes promises without verifiable evidence.

4.2 Comparative Table: Structures and Economic Models

The security of an application depends not only on its technology but also on who controls it and how it makes money.

Application	Ownership Structure	Main Jurisdiction	Economic Model / Funding	Transparency (Code, Audits, Finances)	Potential Impact on Privacy / Conflict of Interest
TeleGuard	Private Company (Swisscows AG)	Switzerland[19]	Donations, Premium ID, Business (future)[18]	Very Low (Closed Code, No Audits)	Medium (Unknown Commercial Objectives)

Application	Ownership Structure	Main Jurisdiction	Economic Model / Funding	Transparency (Code, Audits, Finances)	Potential Impact on Privacy / Conflict of Interest
Olvid	Private Company (Olvid SAS)	France[21]	Freemium (Basic Free, Paid Enterprise) [3]	High (Open Client, ANSSI Audits)	Low (Model Aligned with Privacy)
Session	Foundation (Session Tech Found.)	Switzerland[25]	Crypto ($SESH Staking, Future Premium) [4]	High (Open Code, Quarkslab Audit)	Low (Foundation, Decentralized Model)
Telegram	Private Company (Durov)	Dubai (?)[7]	Durov's Fortune, Premium, Ads (Channels) [29]	Medium (Open Client, Closed Server)	Medium/High (Opacity, Metadata Collection)
Signal	Foundation (Signal Foundation)	USA[38]	Donations, Grants[35]	Very High (All Open, Audits, 990)	Very Low (Non-profit, Aligned Mission)
WhatsApp	Tech Giant Subsidiary (Meta)	USA[40]	Meta Ecosystem (Data -> Ads), Business	Very Low (Closed Code, Data Collection)	Very High (Major Conflict of Interest)

This table clearly shows how structure and funding can influence trust. Signal, with its non-profit foundation funded by donations, presents the least conflicts of interest. Olvid and Session, with their freemium or crypto/foundation model in Switzerland, also seem well aligned. In contrast, WhatsApp, as a subsidiary of Meta whose core business is data exploitation, presents a major structural conflict of interest. Telegram and TeleGuard fall in between, with some opacity or commercial objectives that could potentially take precedence over privacy.

4.3 Detailed Comparative Analysis

- **Encryption**: Signal, Olvid, Session, and WhatsApp (for personal chats) offer E2EE by default, which is the best practice. Telegram and TeleGuard lag behind, with Telegram offering it only as a limited option and TeleGuard using a non-standard, unverifiable protocol. Olvid stands out with metadata encryption, offering an additional layer of protection.
- **Metadata**: This is a crucial battleground. Olvid and Session are designed to collect as little as possible, or none at all in the case of Olvid. Signal actively minimizes their collection. TeleGuard claims to collect none but without proof. Telegram and especially WhatsApp collect a significant amount, which is their main privacy risk.
- **Anonymity**: Session and Olvid offer the highest level of anonymity by not requiring any personal identifiers. TeleGuard follows with its specific ID. Signal has greatly improved with usernames masking the phone number. Telegram and WhatsApp, requiring a phone number, offer the least anonymity.
- **Architecture**: Session's decentralization and Olvid's trustless model offer better resilience to censorship and outages and enhance metadata protection compared to the centralized architectures of Signal, WhatsApp, Telegram, and TeleGuard. However, centralization can allow for better performance and simpler synchronization.
- **Transparency**: Signal is the champion of transparency (everything open-source, regular audits, public finances). Olvid (open-source client, certifications) and Session (open-source, audit) are also very good. Telegram is average (open client, closed server, limited audits). WhatsApp and TeleGuard are the least transparent (closed code, no public audits). Transparency is essential for building trust in security.
- **Structure and Funding**: Signal's non-profit model is ideally aligned with privacy protection. Olvid's freemium model and Session's foundation/crypto model are also well positioned. Telegram's model (premium/limited ads) is acceptable but less transparent. WhatsApp's model is intrinsically conflicted due to its ownership by Meta. TeleGuard's model is linked to a private company whose exact motivations remain unclear.

5. Evaluation for Novice Users: Strengths and Weaknesses

For a novice user, here is a simple summary of the advantages and disadvantages of each application:

- **TeleGuard**:
    - **Strengths (claimed)**: Allows chatting without giving your phone number. Based in Switzerland, a country known for data protection.
    - **Weaknesses (actual)**: No evidence of security (closed code, no known independent tests). Cannot verify if promises are kept. Dubious reliability.
- **Olvid**:

    - **Strengths**: Maximum proven security (even encrypts "who talks to whom," certified by the French state). Very anonymous (no need for a number or email).
    - **Weaknesses**: Less well-known (your friends may not use it). Adding contacts requires a manual step (scanning a code). Some features (group calls) are paid.
- **Session**:
    - **Strengths**: Very anonymous (no need for a number or email). Excellent protection of information about "who talks to whom" thanks to its special network.
    - **Weaknesses**: May be a bit slower than other applications. Calls are less anonymous than messages. You must keep your "recovery phrase" well to avoid losing your account.
- **Telegram**:
    - **Strengths**: Very popular, many fun features (stickers, large groups, info channels). Fast and easy to use.
    - **Weaknesses**: **Not secure by default**. Most discussions can be read by Telegram. You must remember to activate "Secret Chats" (which do not work for groups). Collects information about your usage.
- **Signal**:
    - **Strengths**: Very secure by default (all messages and calls are protected). Very transparent (verifiable code, independent tests). Managed by a non-profit foundation. Increasingly popular. Now allows hiding your number.
    - **Weaknesses**: Required a phone number (less of a problem now). Maybe a few fewer "gadgets" than Telegram.
- **WhatsApp**:
    - **Strengths**: Used by almost everyone, very easy for staying in touch. Personal messages and calls well protected by default.
    - **Weaknesses**: Owned by Facebook (Meta), which collects a lot of information about you (who you contact, when, etc.) for its other services and advertising. Backups of messages are not protected by default. Closed code.

Choosing a secure messaging app often involves navigating between different poles: **maximum security** (which may require more effort or be less widespread, like Olvid or Session), **ease of use and popularity** (which may hide compromises on privacy, like WhatsApp or Telegram), and a **balance** between these aspects (which Signal strives to achieve). There is no universally "best" application, but rather a choice that depends on what is most important to you.

6. Trade-offs and Conclusion

Choosing a messaging application almost always involves making trade-offs between different aspects.

6.1 Inevitable Trade-offs

- **Security vs. Ease of Use**: Enhanced security measures, such as the absence of automatic cloud backups, the need to manually verify contacts, or manage a recovery key, can make the application a bit less convenient in daily use.
- **Privacy vs. Features**: Some practical features, such as friend suggestions based on your contacts or deep integration with other services, often rely on data collection (metadata) that reduces your privacy. Very large open groups or bots can also be less private by nature.
- **Anonymity vs. Contact Discovery**: Not using your phone number enhances anonymity but makes it harder to automatically find your friends who are already using the application.
- **Security vs. "Network Effect"**: An ultra-secure application won't be very useful to you if none of your contacts use it. Sometimes, a "sufficiently" secure but widely adopted application can be more practical.

6.2 Summary Table of Trade-offs

This table summarizes the main advantages, disadvantages, and trade-offs of each application from the perspective of a novice user.

Application	Key Advantages (Security/Privacy)	Key Disadvantages (Security/Privacy)	Major Trade-off (vs. Ease/Features/Popularity)
TeleGuard	Claimed anonymity (no phone), Swiss servers	Complete lack of evidence (closed, no audits), questionable reliability	Strong but unverifiable promises vs. transparent alternatives
Olvid	Maximum proven security (E2EE + metadata, ANSSI), very high anonymity	Smaller user base, manual contact addition, paid advanced features	Maximum verifiable security/privacy vs. lower popularity/convenience
Session	Very high anonymity, excellent metadata protection (decentralized)	Potential slowness, less anonymous calls (P2P), recovery phrase management	Top anonymity/metadata privacy vs. performance/simplicity/call anonymity
Telegram	Rich features, popular, fast	Weak default security (no E2EE), criticized protocol, metadata collection	Features/popularity vs. weak default security/privacy

Application	Key Advantages (Security/Privacy)	Key Disadvantages (Security/Privacy)	Major Trade-off (vs. Ease/Features/Popularity)
Signal	Strong default E2EE security, very transparent, non-profit, good anonymity	Fewer "gadgets" than Telegram?	Excellent security/privacy/transparency balance vs. maybe less "fun" than Telegram
WhatsApp	Extremely popular, easy, default E2EE for personal	Massive metadata collection (Meta), non-E2EE default backups, closed	Extreme popularity/ease vs. very low metadata privacy (Meta)

6.3 Conclusion and Final Recommendations

There is no perfect messaging application that ticks all the boxes for everyone. The choice depends on your personal priorities and your level of concern about your privacy and the security of your communications.

Here are some guidelines to help you:

- **If your absolute priority is maximum, proven, and verifiable security, as well as anonymity, and you are willing to make some effort to convince your contacts or for slightly less immediate use**: **Olvid** or **Session** are the best choices. Olvid offers unique technical guarantees (metadata encryption, no trust in servers) validated by third parties. Session offers robust anonymity and metadata protection through decentralization.
- **If you are looking for the best balance between strong and recognized security, good privacy protection (metadata), high transparency, ease of use, and a significant user base**: **Signal** is very likely the most judicious choice. It has become the reference in reliable and accessible secure messaging.
- **If your priority is to be able to communicate easily with the largest number of your existing contacts, and you accept that Meta (Facebook) collects a lot of information about your communication habits (but not the content of your personal messages)**: **WhatsApp** may be suitable, but **be sure to activate the E2EE encryption option for your cloud backups**.
- **If you are attracted by Telegram's many features (large groups, channels, bots), and you are aware that the default security is weak**: use **Telegram** with caution. **Systematically activate "Secret Chats"** for all your sensitive conversations (remember that they only work for two-person discussions) and be aware of the risks associated with its protocol and metadata collection.
- **Regarding TeleGuard**: In the absence of tangible evidence (open-source code, independent audits) to support its strong security claims, it is difficult to recommend **TeleGuard** based on trust. Its use carries a risk due to this lack of transparency.

Finally, ask yourself: **"What or who do I want to protect my conversations from?"**. The answer to this question (your "threat model") will help you determine the level of security and privacy you truly need. Also, remember to always keep your messaging application and your phone's operating system up to date, as updates often fix security vulnerabilities[43].

7. Simplified Glossary

- **End-to-End Encryption (E2EE)**: A protection method where only the sender and recipient can read the message. The application itself cannot.
- **Metadata**: Information about the communication (who is talking to whom, when, etc.), separate from the message content.
- **Open Source**: The "blueprint" of the application is public, allowing anyone to verify its security.
- **Centralized Server**: All communications go through a central point managed by the company.
- **Decentralized Server**: Communications go through a network of several independent servers, often managed by the community.
- **Security Audit**: An in-depth examination of the application by external experts to find vulnerabilities.
- **Encryption Protocol**: The set of rules and technical methods used to secure messages (e.g., Signal Protocol, MTProto).
- **Anonymity**: The ability to use the application without revealing your real identity (often linked to the phone number).
- **Non-profit Foundation**: An organization whose primary purpose is not to make a profit, often funded by donations (like Signal).
- **Freemium**: A model where the basic application is free, but advanced features are paid (like Olvid).

Sources

1. What is Signal? 7 features that make it a go-to app for private ..., consulté le avril 27, 2025, https://www.zdnet.com/article/what-is-signal-7-features-that-make-it-a-go-to-app-for-private-secure-messaging/ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩

2. Technology - Olvid, consulté le avril 27, 2025, https://olvid.io/technology/en ↩

3. olvid.io, consulté le avril 27, 2025, https://olvid.io/assets/brochures/Olvid_1-page-en.pdf ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩

4. Frequently Asked Questions - Session Private Messenger, consulté le avril 27, 2025, https://getsession.org/faq ↩

5. Is WhatsApp safe? The pros, cons, and hidden dangers, consulté le avril 27, 2025, https://us.norton.com/blog/privacy/is-whatsapp-safe

6. Secure Encrypted Messaging - Defensive Computing Checklist, consulté le avril 27, 2025, https://defensivecomputingchecklist.com/SecureMessaging.php

7. Is Telegram safe for the average user? - Norton Antivirus, consulté le avril 27, 2025, https://us.norton.com/blog/privacy/is-telegram-safe

8. Telegram Encryption: An In-Depth Look at Security in 2024 - Insights For Success, consulté le avril 27, 2025, https://www.kiledjian.com/main/2024/8/30/telegram-encryption-an-in-depth-look-at-security-in-2024

9. TeleGuard on the App Store, consulté le avril 27, 2025, https://apps.apple.com/us/app/teleguard/id1505636751

10. Why not - free messenger, consulté le avril 27, 2025, https://www.freie-messenger.de/en/warumnicht/

11. The Best Private Messaging Apps for 2025 | PCMag, consulté le avril 27, 2025, https://www.pcmag.com/picks/best-secure-messaging-apps

12. Is Telegram really an encrypted messaging app? – A Few Thoughts on Cryptographic Engineering, consulté le avril 27, 2025, https://blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app/

13. Salsa20 - Wikipedia, consulté le avril 27, 2025, https://en.wikipedia.org/wiki/Salsa20

14. The Salsa20 Family of Stream Ciphers - SciSpace, consulté le avril 27, 2025, https://scispace.com/pdf/the-salsa20-family-of-stream-ciphers-4la86gmtaq.pdf

15. TeleGuard app : r/privacy - Reddit, consulté le avril 27, 2025, https://www.reddit.com/r/privacy/comments/1cbyhnd/teleguard_app/

16. Privacy Policy - TeleGuard, consulté le avril 27, 2025, https://teleguard.com/en/privacy

17. SimpleX Chat - the first messaging platform that has no user identifiers - v2.2 of mobile apps with the new privacy and security features just released! - Reddit, consulté le avril 27, 2025, https://www.reddit.com/r/privacy/comments/v4rhch/simplex_chat_the_first_messaging_platform_that/

18. TeleGuard - secure messenger from Switzerland, consulté le avril 27, 2025, https://teleguard.com/

19. Swisscows - Wikipedia, consulté le avril 27, 2025, https://en.wikipedia.org/wiki/Swisscows ↩ ↩ ↩

20. Olvid (software) - Wikipedia, consulté le avril 27, 2025, https://en.wikipedia.org/wiki/Olvid_(software) ↩ ↩ ↩ ↩ ↩

21. Olvid 2025 Company Profile: Valuation, Funding & Investors ..., consulté le avril 27, 2025, https://pitchbook.com/profiles/company/339907-78 ↩ ↩

22. The Security of the Session Messenger – A Guide - Protectstar.com, consulté le avril 27, 2025, https://www.protectstar.com/en/blog/the-security-of-the-session-messenger-a-guide ↩ ↩ ↩

23. Session | Send Messages, Not Metadata. | Private Messenger, consulté le avril 27, 2025, https://getsession.org/ ↩ ↩

24. About OPTF | Privacy is a fundamental right., consulté le avril 27, 2025, https://optf.ngo/about-optf ↩

25. Introducing the Session Technology Foundation - Session Private Messenger, consulté le avril 27, 2025, https://getsession.org/introducing-the-session-technology-foundation ↩ ↩ ↩ ↩

26. The Digital Privacy Paradox: Encrypted Messaging App 'Session ..., consulté le avril 27, 2025, https://www.socpub.com/articles/digital-privacy-paradox-encrypted-messaging-app-session-solves-what-others-wont-18037 ↩ ↩

27. Best Secure and Encrypted Messaging Apps in 2025 - CyberInsider, consulté le avril 27, 2025, https://cyberinsider.com/secure-encrypted-messaging-apps/ ↩ ↩ ↩ ↩ ↩ ↩

28. Is Telegram Safe? A Guide to the Secure Messaging App - Avast, consulté le avril 27, 2025, https://www.avast.com/c-is-telegram-safe ↩ ↩

29. Telegram Privacy Policy, consulté le avril 27, 2025, https://telegram.org/privacy?setln=fa ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩

30. Signal vs Telegram: Security & Privacy Comparison - Cyber Citadel, consulté le avril 27, 2025, https://cybercitadel.com/signal-vs-telegram-a-detailed-comparison-of-security-and-privacy/ ↩ ↩

31. The best encrypted messaging apps in 2025 - Tom's Guide, consulté le avril 27, 2025, https://www.tomsguide.com/reference/best-encrypted-messaging-apps ↩

32. On the CCA (in)Security of MTProto - ResearchGate, consulté le avril 27, 2025, https://www.researchgate.net/publication/310823273_On_the_CCA_inSecurity_of_MTProto ↩

33. Telegram | Overview, History, & Facts | Britannica, consulté le avril 27, 2025, https://www.britannica.com/topic/Telegram-software ↩ ↩

34. Who Owns Telegram Messenger – CanvasBusinessModel.com, consulté le avril 27, 2025, https://canvasbusinessmodel.com/blogs/owners/telegram-messenger-who-owns

35. Is Signal Safe? A Closer Look at the Privacy Messaging App, consulté le avril 27, 2025, https://www.cyberghostvpn.com/privacyhub/is-signal-safe/

36. Tightening up Text Message Security with Signal Private Messenger - Oklahoma Bar Association, consulté le avril 27, 2025, https://www.okbar.org/cm_articles/tightening-up-text-message-security-with-signal-private-messenger/

37. Which app for secure messaging : r/privacy - Reddit, consulté le avril 27, 2025, https://www.reddit.com/r/privacy/comments/1icijvv/which_app_for_secure_messaging/

38. en.wikipedia.org, consulté le avril 27, 2025, https://en.wikipedia.org/wiki/Signal_(software)#:~:text=Signal%20is%20now%20developed%20by,created%20by%20them%20in%202018.

39. WhatsApp Privacy | Secure and Private Messaging - WhatsApp.com, consulté le avril 27, 2025, https://www.whatsapp.com/privacy

40. Top 3 Companies Owned by Facebook (Meta) - Investopedia, consulté le avril 27, 2025, https://www.investopedia.com/articles/personal-finance/051815/top-11-companies-owned-facebook.asp

41. Regular reminder that Telegram's encryption protocol, MTProto, is not secure, an... | Hacker News, consulté le avril 27, 2025, https://news.ycombinator.com/item?id=14375508

42. Olvid for Android - GitHub, consulté le avril 27, 2025, https://github.com/olvid-io/olvid-android

43. Teleguard: Swiss Made Safe Messaging - Hacker News, consulté le avril 27, 2025, https://news.ycombinator.com/item?id=25882319