Application Suggestions

Below are some suggestions for secured messaging platforms for your SmartPhones, along with details concerning each application:

Signal: https://whispersystems.org/

- Traffic encrypted in transit
- Encrypted so that provider cannot read content
- Contacts can be cryptographically verified
- If keys are stolen, past communications remain secure
- Code is open to independent review
- All security/encryption is documented and meets standards
- Both have a recent full code audit
- **Suggested Article:** http://techcrunch.com/2015/03/05/signal-keeps-your-iphone-calls-and-texts-safe-from-government-spies/

Silent Circle: https://www.silentcircle.com/

- Traffic encrypted in transit
- Encrypted so that provider cannot read content
- Contacts can be cryptographically verified
- If keys are stolen, past communications remain secure
- Code is open to independent review
- All security/encryption is documented and meets standards
- Both have a recent full code audit
- **Suggested Article:** http://www.wired.com/2015/09/review-blackphone-2/

Wickr: https://www.wickr.com/

- **From Wickr site**: Wickr is a secure communications company founded on the belief that privacy is a universal human right that enables innovation and economic growth, and empowers democracy. As a security-focused company, we are committed to constantly improving our best-in-class encryption technology against emerging threats that businesses and individual users face daily, protecting their data and communications. To date, we have undergone four public security audits. Each time, our encryption technology — which is the centerpiece of all our products—has received perfect scores from the most prominent experts in the field.
- **Bug Bounty**: As a company of InfoSec experts, we know security is a team sport. Securing the world's communications requires all resources available to us to ensure our code can withstand emerging threats. White-hats, academics, security engineers and evangelists have been responsible for some of the most cutting-edge, eye-opening security revelations to date. The Wickr Bug Bounty is designed to encourage top-notch security researchers to help us identify and mitigate any potential issues in Wickr ecosystem. We pledge to drive constant improvement with the goal of keeping Wickr the most trusted messaging platform for our users.
- **Transparency:** Every quarter, we publish a Transparency Report outlining our current policies and detailing how many government requests we've received in the prior three months. Check their website at www.wickr.com for the report.
- **Law Enforcement:** Our company exists to help individuals and businesses secure their sensitive communications and data. Our tools are, therefore, used by many to discourage and thwart cybercrime. Occasionally, we receive requests from law enforcement for user information. It is important to us to support law enforcement's mission to counter crime within the bounds of the law and to the best of our ability. We require a warrant before handing over the contents of communications. Our encryption technology, however, leaves the contents of any communications we might lawfully release undecipherable.

ChatSecure with Orbot-https://chatsecure.org/

- **From the ChatSecure site:** ChatSecure is a free and open source encrypted chat client for iPhone and Android that supports OTR encryption over XMPP. ChatSecure was originally available for only iOS devices, but is now also available on Android via The Guardian Project's similar app, formerly named Gibberbot.
- ChatSecure is available on the Apple App Store and Google Play Store for free.

Off-The-Record Messaging (Pidgin/Windows): https://otr.cypherpunks.ca/

- **From the Off-the-Record Site:**
- **Encryption:** No one else can read your instant messages.
- **Authentication:** You are assured the correspondent is who you think it is.
- **Deniability:** The messages you send do *not* have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, *during* a conversation, your correspondent is assured the messages he sees are authentic and unmodified.
- **Perfect forward secrecy:** If you lose control of your private keys, no previous conversation is compromised.

Telegram: https://telegram.org/

- **From the Telegram site:**
- **Security:** Telegram is more secure than mass market messengers like WhatsApp and Line. We are based on the MTProto protocol, built upon time-tested algorithms to make security compatible with high-speed delivery and reliability on weak connections. We are continuously working with the community to improve the security of our protocol and clients.

- **Encryption:** We support two layers of secure encryption. Server-client encryption is used in Cloud Chats (private and group chats), Secret Chats use an additional layer of client-client encryption. All data, regardless of type, is encrypted in the same way — be it text, media or files. Our encryption is based on 256-bit symmetric AES encryption, RSA 2048 encryption, and Diffie–Hellman secure key exchange.