

UNPLUGGED PHONE

The Unplugged phone offers robust security features and an intuitive user experience. They make the attempt to collect much less data than competitors, but have contradictory information from what they claim, and what is in their privacy policy.



ABOUT

The Unplugged phone is advertised as a “security and privacy” centric phone, that protects your data. It boasts a multitude of apps already in the phone that include an encrypted messaging system, a VPN with zero-logs, a kill-switch embedded on the phone, a firewall with blockers on Trackers, ads, malwares, adult sites, gambling site, and “Fake news” sites. In its privacy center you can also block unsecured WiFi networks, Bluetooth, outgoing NFC (Near Field Communication), camera access, location access, and USB data transfer. They also state that their servers are in international waters, connected to Starlink via satellite, claiming that makes them not subject to any governmental law.

DATA COLLECTED

1. Financial Data

- **No Sale of Data:** Unplugged asserts that they do not sell collected data to third parties.
- **Payment Processing:** They utilize third-party services for payment processing, meaning your financial data will be subject to those third parties' privacy policies.
- **Types of Collected Information:** They collect various personal details, including registration information, data from Messenger and VPN usage, support inquiries, and information used for service improvement.
- **Fraud Prevention and Security:** They may use this data to detect and prevent fraud and enhance the security of their services.

2. Personal Information

- **Disclosure of Information:** The company claims they will try not to disclose personal information to third parties without consent, except as legally required or specified in the policy.
- **Sharing with Third Parties:** They may share your information with affiliates or subsidiaries, and this could involve entities in different countries, which may have varying data protection standards.
- **Corporate Changes:** Your information could be transferred in the event of a merger or sale of assets, which is common in corporate transactions.
- **Legal Compliance:** Even if their servers are located in international waters, they state that they can disclose information to comply with legal requests like subpoenas or court orders.
- **Opt-Out Options:** They provide a way to opt out of certain data sharing, which is a good practice for user control over personal information.

OTHER AREAS OF CONCERN

If you download apps such as Facebook, Instagram, or X onto the phone, those companies still retain the rights to collect the data they set forth in their terms and conditions. You may be able to limit some of those things with the phones built in privacy, but you can do most of the same with iPhone or Android.

This phone is not “impenetrable” by any means. The Unplugged phone is still susceptible to cell phone triangulation based on tower data, even with your location data turned off.

Not all of their server farms are located in international waters as stated. Other locations include Israel, Cyprus, Iceland, Switzerland, Liechtenstein, UAE and other undisclosed locations.

Unplugged's technology operation are run by Eran Karpen, who worked in cyber security / espionage and was involved in the Pegasus software.

ENDING NOTES

The Unplugged phone is not a worthwhile investment. Its features overlap with those offered by both Apple and Android devices, meaning there's no significant advantage in choosing it over more established options. While the unplugged phone does have less aggressive data collection practices compared to its competitors, this doesn't make it completely secure. If you plan to add your everyday apps to it, you'll still be exposing your personal information to potential risks.