



Federal CyBi-Safe Mobile Carrier Compliance
(Preventing Child Exploitation)

Anonemis Research
Símenona Martínez
AnonemisResearch.com

Federal CyBi-Safe Mobile Carrier Compliance

Preventing Child Exploitation

Federal policy and practice standards to be updated with compliance of all mobile carriers requiring that users complete cyber-safety training and user CyBi-safe compliance agreement upon registration of all devices. User confidentiality is of the utmost importance which is why A.I smart machining is the first line of defense in protecting citizen privacy in the fight against child exploitation.

Processes and Procedures

All minors must have corresponding agreement and permission with digital signatures with/from legal guardians, who are also required to read an overview and answer questions regarding carrier and device agreements with CyBi-Safe software in effort of preventing child exploitation.

Users who are minors are required to have an added encryption and filter feature which prevents nudes and/or private credentials from being distributed or received by an additional encrypted interception which auto flags high-risk content with utilizing smart A.I machining software download, required upon registration in all minor operated devices.

Telecommunication efforts comply by monitoring numbers who engage in abnormal behavioral activities at rapid pace, packet flooding, denial of services, spamming, catfishing, and other cyber criminalities.

- Detecting mobile devices who exchange large quantity of high-risk content concerning nudity, particularly in minor registered devices and credentials.
- Those numbers are to be flagged for monitoring and detained in federal quarantine for further inspection.
- Numbers registered with suspicious area codes and pinging from towers outside of approved geographical area of the minor's location are automatically flagged, in an effort in preventing sextortion, kidnapping, cyberbullying, and sex-trafficking.

These suspicious numbers are held in federal quarantine where reserve engineering can be engaged, by distributing Spider Malware for additional monitoring and inspections.

This process and procedures aid in establishing the sourcing and identifying the players within these criminal enterprises in the child trafficking, extortion, and overall exploitation.

Cellphone carriers should also auto-populate suicide resources anytime the word is mentioned in text exchange.