No images? Click here

Can You See Me Now?

An Overview of Secure Messaging Applications

by Brian J. Kelly - Supervisory Cyber Analyst

End-to-end encryption, self destructing messages, remote lock and wipe, and restricted sharing are all features touted by a number of secure messaging applications available for anyone (not just CIA assets) to download and use. But do you know what these features do? Do you need them? Is a person under your supervision using a secure messaging application? Is that a concern?

There is no shortage of applications advertising as "secure messaging" platforms. The most widely used of these applications is WhatsApp, which is owned by Meta (which also owns Facebook and Instagram). Other well-known secure messaging applications are Telegram and Signal, but this space also includes applications like Wickr, Threema, Element, Confide, Dust and Wire. What makes each of these different? What makes them the same? Some applications are commercially owned, for example, Wickr is owned by Amazon who has decided to close down the application at the end of 2023 (see below). Others are open source, such as Threema, Wire and Element. The majority of these applications all advertise similar features, which are explained in more detail below.

End-to-end encryption (E2EE): Any data transmitted by the service is encrypted by the sender device and only that device and the receiver device hold the cryptographic keys. The application's server simply acts as a bridge, passing along messages that itself can't decipher. It is noted that E2EE will be a default feature on Facebook Messenger by the end of 2023, The encryption should be AES compliant (Advanced Encryption Standard). AES was initially established by the U.S. National Institute of Standards and Technology (NIST) in 2001. 256-bit refers to the length of the key used to encrypt the information and is virtually unbreakable by brute force (as per 2023 computing power). Because of this, it is considered the strongest encryption standard to-date.

Self-destruct: This feature will allow a message to delete itself after being read. Some services allow the sender to set a predetermined amount of time before the message self-destructs. Some providers do maintain these destroyed messages on company servers.

Restricted sharing: Some platforms prevent users from sharing or saving any media delivered via the app. This prevents any sensitive data leaking out beyond the intended communication.

Remote lock & wipe: The user is able to remotely lock access to the messaging platform, in order to safeguard sensitive data. The user can also send a remote command to wipe all data from the application.

With these robust privacy and security features, secure messaging applications unfortunately attract the use of the platforms for nefarious purposes. From the use by foreign and domestic terrorist organizations, to the sharing of child sexual abuse material on channels and groups within the application, the privacy features make it difficult to track the users engaging in this behavior. Such features also make users of these platforms targets for various scams. See below for recent news stories on the use of secure messaging applications to facilitate criminal behavior:

TV news producer repeatedly distributed child porn in Telegram group ominously named 'The Playground Lives': FBI
Jerry Lambe - Law & Crime
https://lawandcrime.com/crime/tv-news-producer-repeatedly-distributed-child-porn-in-telegram-group-ominously-named-the-playground-lives-fbi/

St. Louis man admits to transporting child sex abuse images, fleeing city while on house arrest
Clarissa Cowley - KSDK
https://www.ksdk.com/article/news/crime/st-louis-child-sex-abuse-images-florida/63-f7bb916e-ecb1-4f15-864b-5072a4c27cc1

Wickr Me, Amazon's encrypted chat app, stops accepting new users
Ben Goggin - NBC News
https://www.nbcnews.com/tech/tech-news/wickr-me-shut-down-new-user-amazon-encrypted-chat-app-stops-rcna63536

Sex offender deleted secure messaging app from phone before police could check it
Jason Evans - Wales Online
https://www.walesonline.co.uk/news/wales-news/sex-offender-deleted-secure-messaging-27399229

Somalia Suspends TikTok, Telegram Amid Terrorism Fears
Abubakar Idris - The Messenger
https://themessenger.com/tech/somalia-suspends-tiktok-telegram-amid-terrorism-fears

How to Spot a WhatsApp Scam
Gaurav Shukla - How-To Geek
https://www.howtogeek.com/892109/how-to-spot-a-whatsapp-scam/

The use of a secure messaging application by a person under supervision does not automatically mean that person is using the application for nefarious purposes. But agencies and officers should know the features and potential concerns that come with each application, and if applicable, what can and cannot be captured by computer/Internet monitoring technologies. And because this landscape continues to change and evolve, it is essential to keep current on new developments.

IPPC Technologies continues to strive towards predictive and proactive solutions so officers can intervene early, address areas of concern and change behavior. For more information on IPPC's services such as Spotlight, please call IPPC at (888) WEB-IPPC. For any questions/feedback on this or previous article topics, feel free to contact me directly at bkelly@ippctech.net or by calling (516)341-4201. Links to past articles can be found on my personal website.

New and existing clients using Spotlight will soon be able to participate in a monthly Spotlight Feedback Group virtual meeting to obtain a brief overview of the service, current updates and trends, and have the opportunity to pose any questions or comments to the Spotlight team. If you are interested in participating, please email Brian Kelly for more information. Our clients can also give feedback on the service at any time by taking the Spotlight Performance Survey by clicking here.

IPPC TECHNOLOGIES
PO BOX 60144
KING OF PRUSSIA, PA 19406
TEL: 888-WEB-IPPC (932-4772)
INFO@IPPCTECH.NET
WWW.IPPCTECH.NET