Published on *The National Law Review* https://natlawreview.com

# False Sense of Security with End-to-End Encryption

Article By:

Womble Bond Dickinson Communications, Technology and Media

Finding comfort in products that display commitment to both privacy and information security is understandable. The Mobile Ecosystem Forum, a global mobile trade association, published a study that indicated that 49% of the 15,000 survey respondents said a lack of trust limits the number of applications they download.

This makes it all the less surprising that consumers around the world turn to end-to-end encrypted mobile applications to protect their messages, photos, videos, voice messages, documents, status updates and calls. End-to-end encryption means that only the sender and recipient(s) can see messages exchanged.

The process of end-to-end encryption entails converting message into unintelligible pieces of data the moment the user sends it. This message does not become intelligible again until it reaches the recipient's device. However, data flows beyond the vessels of communication. If you store messages on multiple devices, or back up data into a cloud, the security given by end-to-end encryption borders on irrelevance.

We have rather infamous examples of people ignoring the holistic privacy picture based on their use of end-to-end encryption. Paul Manafort, President Trump's former campaign chairman, was accused of witness tampering after trying to hide his communications with potential messages using WhatsApp, an end-to-end encrypted messaging application. Because his phone settings enabled his messages to automatically be backed up in his cloud service, the FBI was able to access these messages. Recent news reports tell us that senior government officials in multiple U.S. allied countries were targeted, and had their phones taken over by breach of their WhatsApp application.

How can we be blamed if we as consumers fall into that same sense of false security as those with influence and power? Their stories should be a wake-up call to take the steps necessary to understand the functions and features of our technology. Protecting your information requires looking at the entire flow of your data. Further, you have to understand and inspect how each application, even the most apparently safe, interact with the rest of the services made available to you.



National Law Review, Volume IX, Number 311