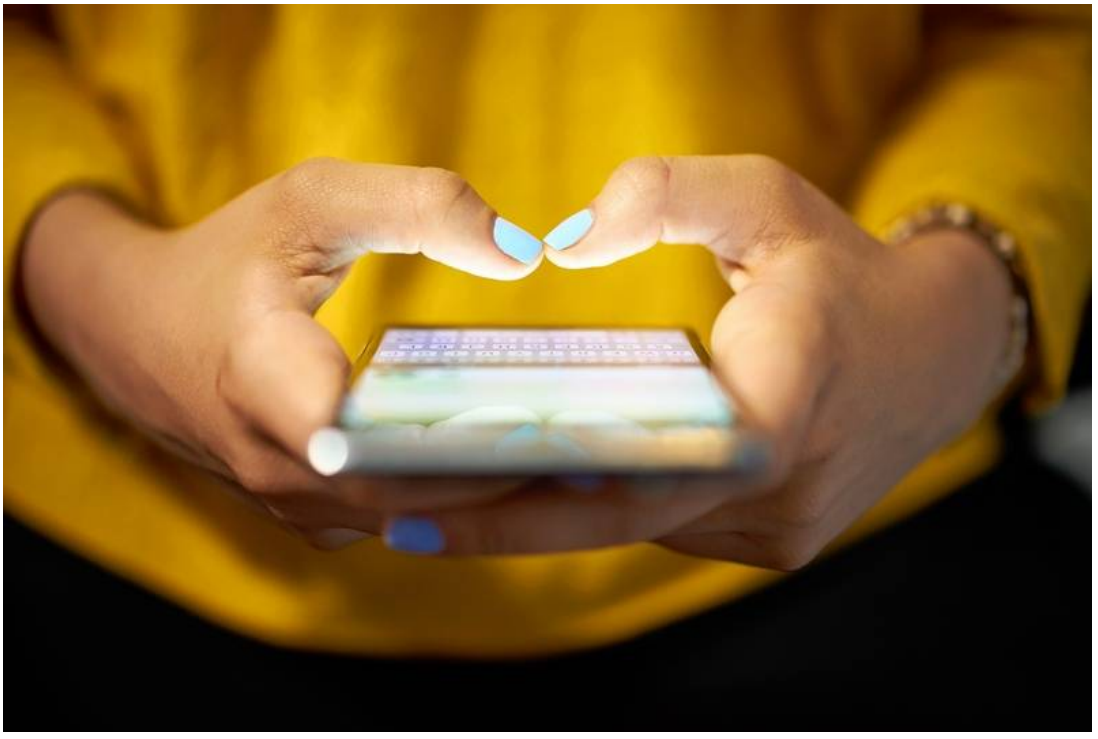
Sections

Daily Herald BUSINESS LEDGER

The Business Resource for Suburban Chicago

News | updated: 9/12/2018 7:42 AM

Why you should think twice about texting your clients



Messaging apps come with varying degrees of encryption; some require manual enabling by both users while others, like iMessage, only offer encryption on iOS, leaving messages to Android users unencrypted. **Davi**

The pace of communication in the professional world increases exponentially daily. Clients used to communicating via text and messaging apps have come to expect that same speed while conducting business and conferring with their legal team. Every business in every industry is trying to find ways to keep up.

Professionals and clients looking for easy, expedient means of communications have turned to mass market messaging apps. But those messaging apps come with varying degrees of encryption; some require manual enabling by both users while others, like iMessage, only offer encryption on iOS, leaving messages to Android users unencrypted.

Lawyers using them to communicate with and about clients are, perhaps unknowingly, putting themselves and their clients' information at risk of being hacked. Not only does nonsecure communication put them at risk ethically, it also puts them at risk financially. A recent study by Ponemon Institute and IBM Security found that the average cost of a data breach for companies in the U.S. was $7.91 million.

While your company might not face that figure, there is still plenty on the line when it comes to leaving data unsecured -- your brand is at risk -- think Equifax and Yahoo.

That risk of data breach has caused some industries to turn toward other encrypted ephemeral messaging options, where messages are deleted after they are read or a set amount of time has passed, in order to prevent their information from being hacked. This kind of self-deleting technology is also present in consumer apps like Snapchat.

It's easy to understand why companies feel the best way to protect their data is not to keep it. But, while that eliminates some vulnerabilities, it also creates new ones.

Because ephemeral messaging systems, by definition, don't create a trusted record of messaging, they leave firms and companies at risk of future complaints and lawsuits from clients and leave both parties vulnerable to the other stealing or misusing the information discussed but then deleted. Without evidence to prove ownership of an idea or comment, it's difficult to rebut those claims.

Ephemeral messaging apps are already accused of wreaking havoc in the tech world. Uber and Alphabet, the parent company of Google and self-driving auto company Waymo, recently settled a $245 million legal battle over the use of one such app used to transfer huge quantities of trade secrets without creating a paper trail.

And there's another, potentially even bigger, question brewing in the legal community: could companies using these apps and failing to preserve their messages be held responsible for destroying evidence?

Laws and regulations on the books at the federal, state and local levels require certain types of companies to maintain various types of documentation. And, federal court decisions also require companies under threat of lawsuits to save all of their electronic documents and, if asked, hand them over in the discovery process.

Even if your company is preserving your text messages, there's always room for human error. In 2016, a Colorado judge held a company responsible for a low-level employee accidentally deleting their text messages -- leaving them out of discovery

So, while most companies are not likely to face a lawsuit like those mentioned, using the same types of nonsecure non-recorded communication technology still leaves them highly vulnerable to costly lawsuits.

Texting provides efficiency. Ephemeral messaging provides protection from data breaches. But both come with drawbacks. Retain your messages and your peace of mind by setting up policies and procedures to ensure that your business is covered. Companies looking for a way to communicate with their clients via messaging apps need to find one that offers a secure method of mobile information exchange and most importantly an archived record of communications to retain for their files -- for their sake, and their clients'.

• David M. Buddingh is president and general counsel for Encrypted Information Exchange LLC, developers of EIE Legal, an encrypted messaging app. He may be reached at DMBuddingh@EncryptedInfoExchange.com or visit EncryptedInfoExchange.com (http://www.EncryptedInfoExchange.com).