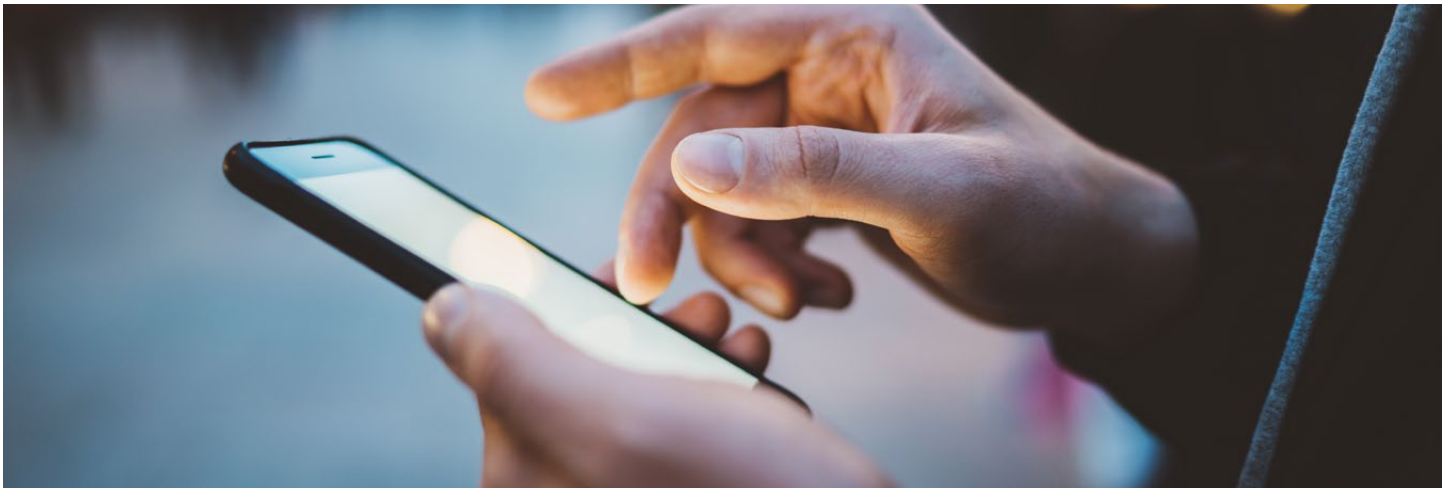


Data Security and Dictation Efficiency Can Go Hand-in-Hand

FLORIAN SCHWIECKER
Leader of Global Sales, Vice President and Director Speech Processing Solutions

It is probably no surprise that a 2016 American Bar Association survey found that more than 93 percent of attorneys use smartphones in their practices. What may raise eyebrows is that 73.6 percent of lawyers who participated in the survey report they were using a personally owned smartphone, while only 28.5 percent used a smartphone that the firm owned.

> "When firms are exploring their mobile and office-based voice technology options, they need to ensure that the functionality is similar to dictation tools attorneys are accustomed to."

Bring your own device (BYOD) policies raise data security and client confidentiality concerns depending on how attorneys protect their devices. Attorneys use their personal smartphones not only for client-related email and text messages, but also to dictate client letters or confidential memos. A lost or stolen smartphone without the proper security features in the hardware and software means valuable, protected client information could be held hostage by a cybercriminal, damaging the reputation of the client and the firm.

Those types of risks should prompt firms to explore secure mobile dictation technology options and associated BYOD policies. Attorneys and their assistants can then enjoy the productivity of working from any location, as well as the robust security necessary to protect clients' confidential and private information and the firm's reputation.

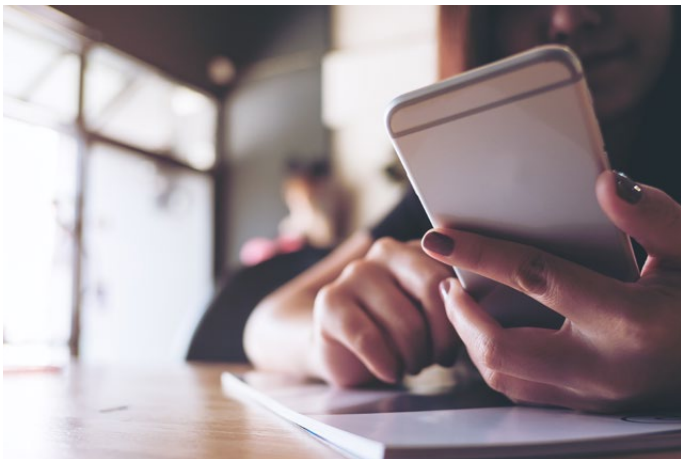
MOVING TO THE CLOUD

One such security-focused option is migrating more data and systems to the cloud, which is a fast-moving trend for organizations. A survey from the International Legal Technology Association found that 62 percent of law firms were "increasing likelihood of adoption" of cloud-based solutions in 2016, up 11 percentage points from the previous year.

The cloud is proving to be a highly efficient and secure platform for data storage and an important tool for supporting law-firm workflows. Document creation, for example, can be

managed entirely from the cloud. Attorneys can dictate either at the firm, from their smartphone or from a handheld recorder at their home, then transfer the recordings to the cloud. From there, cloud-based dictation workflow management systems offer options for how those documents are created. The most common method is for the attorney's assistant to access and even transcribe the recordings in the cloud. The completed documents are securely stored in cloud for the attorney's review.

Increasingly, attorneys are choosing speech recognition software or using transcription services to create their documents. Some smartphone dictation apps enable users to upload their audio files directly to the cloud to either assign to a transcriptionist or process the completed dictation within the cloud. Using either method, the document is created in a few moments, and the attorney simply needs to review and edit before sending to the client.



SECURITY ON THE GO

Secure cloud options are essential for protecting these recordings and documents. After all, 80 of the 100 largest firms in the United States have been hacked since 2011, and 80 percent of respondents to a legal survey consider cyber/privacy security to be one of their firm's top 10 risks. Careful technology selection and policy concerning permitted software and hardware should be a priority for firms concerned with security.

Here are a few security features to consider when designing the firm's BYOD or mobile device policy:

- **End-to-end encryption:** Dictation recorder apps for smartphones should encrypt dictations in real time using the advanced encryption standard (AES or Rijndael algorithm) with a key length of 256 bits. Dictation files should be encrypted again when they are sent to the cloud, and again when stored. This end-to-end double encryption is essential for protection from unauthorized access.

- **Server mirroring:** Not only should stored data in the cloud be automatically encrypted, but the cloud platform should also offer server mirroring to keep data reliably secured and accessible to the firm anytime and anywhere.

- **Passcode options:** Fingerprint and numerical passcode options are common on most smartphones to protect your data. Some handheld digital recorders also offer a PIN option to protect against unauthorized use or file playback.

CONVENIENCE TO SUPPORT EFFICIENCY

These mobile devices and apps used for dictation allow attorneys to create documents and save their thoughts from anywhere without taking the time to type them. Although this can increase firm productivity and improve client service, attorneys will not employ these mobile options if the security policies or features make the technology difficult to use.

When firms are exploring their mobile and office-based voice technology options, they need to ensure that the functionality is similar to dictation tools attorneys are accustomed to if they are experienced dictation users. If the attorneys are new to dictation, a simple user interface is important to shorten any learning curve associated with the new technology.

With highly intuitive — but powerful — voice technology and effective security features, law firms can experience the efficiency of mobile-enabled workflows with safeguards to protect client information and the firm's reputation. ■

ABOUT THE AUTHOR

Florian Schwiecker is the Leader of Global Sales, Vice President and Director at Speech Processing Solutions.

info.na@Speech.com
www.Speech.com
twitter.com/fschwiecker