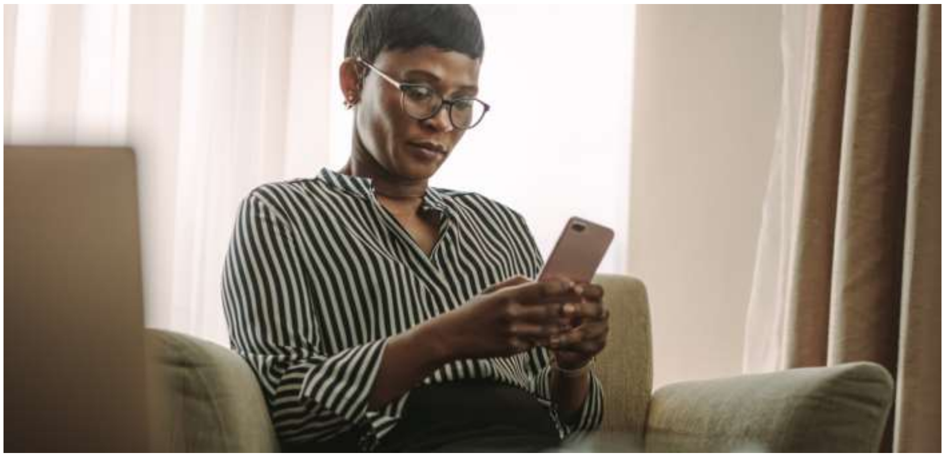
Search...

Law Practice Today

CURRENT ISSUE PAST ISSUES SUBSCRIBE CONTACT ABOUT

YOU ARE AT: Home » Articles » Texting: Your Next Big Vulnerability



Texting: Your Next Big Vulnerability

BY RANJI RAGBEER ON DECEMBER 14, 2021 ·

It’s hard to imagine conducting business without a smartphone. Few of us could function effectively without instant access to email, text messaging, the internet, or a growing number of essential business apps. They’ve permeated every facet of our personal and business lives, to the point where “a staggering 65.6% of Americans check their phones up to 160 times daily.”

Some of the most widely used types of smartphone apps are messaging apps. In 2020, mobile users in the U.S. sent 2.2 trillion texts (up from 1.5 trillion in 2017). With such widespread use, there is little doubt texting will become an integral form of communication for legal practitioners. But there are challenges, some of which are exacerbated by another growth trend: the “bring your own device” (BYOD) movement, where employees use their personal devices for business. The value of personal devices in use for business is forecasted to reach $367 billion in 2022 ($235 billion will be attributable to smartphones) and signs indicate BYOD will become increasingly acceptable in the legal industry.

Unfortunately, if not properly implemented, text messaging can leave legal practitioners vulnerable to a number of professional and ethical risks, especially with BYOD organizations. This article will provide a basic primer on text messaging and explore practical steps to mitigate associated vulnerabilities and risks.

Background

Let’s first explore the broad categories of texting options and the differences between providers and platforms.

THIS ISSUE OF LP TODAY

The Technology Issue | December 2021

- **SMS:** SMS is an acronym for "Short Message Service." While these messages are limited to only 160 characters, SMS is the most widely used messaging method, presumably because SMS apps are delivered with virtually all mobile phones. When an SMS message is sent, it gets transmitted to the nearest cell phone tower before being relayed to an SMS message center (SMSC) which then transmits it for delivery to the cell tower nearest to the recipient. SMS messages are unsecured in transit and while stored at SMSCs, so messages can be read by anyone intercepting the message in transit, or on the SMSC provider's systems. There may also be potential costs depending on the user's mobile plan.
- **MMS:** MMS can be thought of as an SMS sibling. The acronym stands for "Multimedia Messaging Service." It allows SMS users to send multimedia content and messages longer than 160 characters up to a size limit determined by the provider. There is no significant difference between SMS and MMS in terms of their security limitations, but there may be an increased cost for MMS as compared to SMS.
- **iMessage**: iPhone, Mac, and iPads (all on the Apple iOS operating system) use the proprietary iMessage messaging platform. iMessage also supports sending and receiving messages from SMS/MMS users on other platforms. iMessages sent to other Apple users are encrypted both in transit and at rest, so no one intercepting an iMessage message would be able to read iMessages without your passcode. However, iMessages exchanged with an SMS user are not encrypted and have the same security vulnerabilities as SMS. Apple users can also backup iMessages to Apple's iCloud service, which helps keep Apple's user data and applications synchronized, up-to-date, and backed up. But while backups of iMessages to iCloud are encrypted, Apple receives a copy of the backup encryption key. This means that Apple can technically read iMessages backed up to iCloud.
- **Over-the-Top Messaging (OTT):** OTT refers to third-party instant messaging services (or online chat) provided by software and technology providers independently of mobile network operators. They typically are a far more functional alternative to iMessage and SMS, with extended features such as voice calling, video calling, and more. Unlike SMS, OTTs do not need a mobile network to function but do require an internet connection and (in some cases), a mobile data plan. Examples include WhatsApp, Facebook Messenger, Signal, Viber, WeChat, Skype, Telegram, and a host of other providers all offering products that improve the messaging experience. They can be classified into two broad categories: consumer-based messaging, and enterprise-based messaging. The former class is intended for general public use (typically free), while enterprise-based messaging systems are designed for business use (typically at a cost). Most offer end-to-end encryption, and some allow messages to be exchanged (insecurely) with SMS users. Consumer-based messaging systems are highly likely to be used by BYOD users for business. Research shows that 58% of employees in the U.S. admitted to using instant messaging and texting to share sensitive and business-critical data.

One major drawback to using consumer-based OTT systems for business is that the majority require both parties to be members of their community to work. This limits their utility in businesses, where new clients and new relationships are constantly being formed. In addition, many collaboration and application-specific solutions embed messaging in their platforms, such as Microsoft Teams, Slack, and Zoom, but not all support SMS.

Within the legal community, SMS and iMessage are more widely used than OTT systems, but unfortunately, neither of them is designed to address the stricter professional needs of the legal industry. Similarly, consumer-based OTT systems are not designed for professionals either, so careful consideration should be applied if any of these platforms are to be used for communications by legal professionals for business.

Challenges

Undoubtedly, many lawyers happily exchange business-related SMS, iMessage, and consumer-based OTT text messages with clients. The practice is perfectly understandable—text messaging is fast, personal, short, and convenient—all of which are entirely desirable in a fast-moving profession. However, with the rise of BYOD, text messages are increasingly sent to a lawyer's *personal* mobile phone. Consequently, their firm's access to those messages will likely expose the lawyer's personal messages to the firm, creating a privacy risk while raising many important questions and issues with respect to:

IN THIS ISSUE

- data ownership
- data rights
- preservation of the attorney-client privilege
- confidentiality
- records retention
- privacy
- transparency
- and a series of other considerations.

To specifically understand the BYOD risks, consider the many issues that would arise if an employee were to use their personal email address for business. With respect to business emails, the business would have no access, control, monitoring, or records retention capabilities. Additionally, consumer-based email platforms don't have a substantive obligation to protect user data. For the vast majority of businesses, the idea of our employees using their personal email for business is unimaginable. Yet, for millions of businesses, text messaging on personal devices is accepted, even though the potential risks are not dissimilar to using the employee's personal email address for work.

Additional BYOD risks may be imminent, especially if a business requires employees to disclose personal phone numbers for business use. As more and more people abandon landlines, such disclosure is not far removed from disclosing one's home number, introducing additional employee privacy issues and risks as hackers can use mobile numbers for identity theft. A recent article at TechCrunch.com stated:

> "You might think your Social Security or bank account numbers are the most sensitive digits in your life. Nowadays, hackers can do far more damage with little effort using just your cell phone number."

In another article, *New York Times* lead consumer technology writer Brian X. Chen wrote:

> "If you have business cards with your personal [mobile]number printed on them, shred them…"

The problem is likely to get more challenging as privacy laws change, ostensibly in favor of the individual. All signs point to users being careful of protecting their personal mobile phone numbers from broad exposure, which includes sharing personal phone numbers for business as well.

Mitigating the Risk

Texting risks are most commonly addressed using a combination of general communications policies and technology; these serve as "bookends" around the problem. The most widely used technologies are Mobile Device Management (MDM) systems that can be enabled with a wide range of security features, such as remotely controlling a mobile device (including BYOD smartphones). Together, well-written policies and MDMs are highly defensible and provide adequate protection for most situations. When drafting internal policies that cover text messaging, several recommended policy and technology considerations should be explored.

Policy Considerations

- **Employee privacy**. If employees use their personal devices for business, what expectation of privacy should the firm set (if any)? While it's widely accepted that employees should have no expectation of privacy when using company-issued equipment or resources, there are still some grey areas with text messaging in BYOD organizations. Unlike the firm's email address, BYOD texting is a bit more challenging precisely because employees are using their own phone numbers for personal and business purposes. My organization is currently working on technology that clearly separates business from personal communications and data (including text messaging), with the goal of giving the organization control and transparency to legitimate business communications, without compromising employee privacy. Regardless of whether your organization has such technology or not, the firm should clearly identify the organization's rights to collect, monitor, review, and store text messages sourced from a personal device used for work purposes.

- **Confidentiality**. Due to the nature of SMS texting, policies should set clear guidelines for text message transmission of confidential and sensitive business information. There is a vast difference between a text message stating "I'll be there in 5 mins" versus one that states "Should we offer to settle for $25 million?" In the second instance, the user should be aware that the transmission is not secure and carefully weigh the risks involved. Accordingly, appropriate employee training on permissible text message usage and approved platforms is highly recommended.
- **Records retention.** For most BYOD organizations, text message records retention is a consequential if not a burdensome "art." There is no legal or technical reason why all text messages on a personal mobile device cannot be archived subject to properly drafted company policies. However, while a number of solutions on the market can archive SMS messages, employees may shudder at the notion of their personal text messages forever being part of the company archives. This is one area that many organizations (including my own) are working to address with innovative technology that can separate business and personal text communications for record-keeping and operational purposes. Separation helps respect the employee's privacy rights while giving organizations transparency to data they are entitled to access.
- While policies are essential, having a compliance monitoring tool to review and monitor text message compliance with the organization's policies and regulatory requirements (where applicable) is also advisable. The range of compliance monitoring tools is extensive, and implementation requires a good understanding of the limitations of the technology to properly configure and manage any such system. Properly deployed, a compliance monitoring tool can provide an added layer of security and oversight that may be highly appropriate in some business environments.
- **Online back-up.** Mobile phones can be easily backed up to the cloud. If an employee chooses to back up their mobile devices to an online service, business text messages will also be stored, possibly beyond the reach of the organization. In such cases, if there is a need to recover the data, how will the organization exercise its right?
- **Attorney-client privilege**. Lawyers who correspond with clients via texting should remember that those messages are not (except as noted previously) end-to-end encrypted. Implementing a strict protocol governing the appropriate use of text messaging with clients is advisable to protect and preserve the attorney-client privilege.

Technology Considerations

- **MDM Technology:** This is complex technology. Relative to text messaging, the most important MDM attribute is their ability to protect information and apps if a mobile device is lost or stolen, or upon separation of an employee from the organization. Common MDM features include:
  - Device security (data encryption, access monitoring, security configuration, and more)
  - Network accessibility (managing secure access from the device to the organization's network)
  - Remote configuration and troubleshooting (ability to deploy and configure mobile apps remotely)
  - Remote wiping (ability to remove data from a mobile phone remotely if lost or stolen)
  - Device location tracking (allows the MDM to track/find a device remotely)

Although the above are common features found in most MDMs, not all will be necessary for all law firm users. Typically, they are highly configurable, making it relatively straightforward for organizations to choose which functions would be most appropriate for their environment and specific classes of users.

- **Emerging Technologies:** Technology is changing rapidly. Technology companies are working diligently to leverage texting to the advantage of law firms and law departments by eliminating inherent risks. These systems will also introduce features and functionality appropriate for professional use with the same ease-of-use and convenience of OTT consumer-oriented messaging systems. Some of the problems being addressed by my company include:

- Delivering world-class encryption without requiring the external party to use the same app as the OTT user
- Separating business and personal communications on the same device so organizations gain transparency and control without compromising employee privacy. Separation also facilitates other desirable business processes such as records retention, information governance, and compliance, while addressing concerns such as confidentiality and the attorney-client privilege.
- Centralized account management control and monitoring
- Contact-centric (as opposed to app-centric) organization of all communications on the smartphone
- Integration with compliance, early case assessment, litigation avoidance, document management, marketing, and other tools thereby allowing the organization to gain full control of text message assets.

Our end goal is to fully incorporate text messaging into a professional's communications arsenal, but in a manner that largely eliminates text messaging risks by giving organizations information governance control, while respecting employee privacy.

The Bottom Line

Without question, text messaging is a useful tool for business. Legal practitioners, however, have an added professional and ethical obligation to use the technology responsibly. With the right combination of policies, technologies, employee education, defensible practices, and strategies for evaluating new technologies and emerging privacy legislation, law firms and other legal providers can substantially eliminate text messaging vulnerabilities while building stronger business relationships, increasing employee satisfaction, and protecting valuable organizational know-how and information assets.

About the Author

Ranji Ragbeer *is the principal at Tendant, a provider of a marketing and communications platform for smartphones. For over 35 years, Ranji has worked on many legal technology "firsts," and is currently working on improving smartphone information governance.*

Ramón Viñas-Bueso, Viñas Law Office LLC

Susan White, Mass LOMAP

About ABA Law Practice Today

Advertise

Contact

Information

New Law Anthology

Submit a Pitch

Syndicate

Current Issue · Past Issues · Terms of Use · Code of Conduct · Privacy Policy · Your Privacy Rights · Your California Privacy Rights · Copyright & IP Policy · Advertising & Sponsorship ·