Tech-Powered Communication: Boosting Efficiency and Ensuring Security

Advancements in communication technology have increased both choices and challenges, including concerns about privacy and security. Here's what lawyers need to know.

BY JAMES PEARSON

Communication technology has evolved significantly over the past decade. During the global pandemic, a wide range of communication options became more popular, such as the videoconferencing platforms Zoom, Teams, and Google Meet, and their use has continued. Once reserved for comic books and science fiction, video calling and portable communication devices have become ubiquitous.

Phones have evolved from landlines that kept people tied to a cord and a single location to internet-integrated voice over IP (VoIP) solutions. Long-distance calling plans have become obsolete, and instantaneous communication through email, web fax, texting, and various social media platforms is now the norm. With these advancements come both choices and challenges, including concerns about privacy and security.

New communication technologies offer significant advantages despite their complexities and security challenges. They allow for asynchronous communication, making it easier to work across various settings, including remote environments, without the limitations of time zones. Such flexibility expands customer bases and talent pools and levels the playing field between small businesses and large corporations while keeping costs manageable. Moreover, these technologies enhance disaster recovery capabilities and can improve resilience, ensuring your business continues operating or is able to return to operation with minimal downtime. However, it's crucial to remain vigilant about the potential drawbacks associated with these technologies.

The Power of Collaborative Communication Tools

Videoconferencing technologies have transformed work environments, providing cost-effective solutions for global communication. Teams, Microsoft 365, and other platforms enhance collaboration through features such as document sharing and instant messaging, making communication more efficient than ever.

Prospective and current clients increasingly reach out via websites, social media, or text messaging. Instantaneous communication and multiple ways of communicating with lawyers have become the expectation.

Phone Apps. Mobile apps linked to VoIP systems significantly boost communication efficiency, allowing users to handle business calls and messages on their devices effortlessly. Using a mobile application from a VoIP provider transforms a smartphone into a portable office. A VoIP solution may also intelligently reroute

James Pearson owns the Computer Center, Janesville. He is a Microsoft Certified Professional and a frequent author and speaker on cybersecurity and safety topics. Access the digital article at www.wisbar.org/wl.

james.pearson@computercenter.com

www.thelawyersgeek.com

calls to the recipient, no matter where that person is.

Moreover, phone apps offer a strategic advantage by enabling personal devices for professional communication without exposing private numbers. The apps disguise the private number, displaying a work phone number instead. Even if the work number initially was assigned to a desk phone, these apps provide the capacity to send and receive text messages, along with features like call recording. This combination seamlessly integrates the convenience of personal devices with the professionalism of work-related communication.

Collaboration Tools. In addition to the evolution of oral and visual communication methods, collaboration tools like Google Workspace and Microsoft 365 have revolutionized work. These platforms enable users to edit documents, share them globally, and dispatch them via email in a fraction of the time it once took. Microsoft Teams emerged as a central hub for internal and external communication and collaboration, streamlining interactions within offices and with current and prospective clients.

Email. Despite significant technological advances, email continues to be a core component of most people's communication toolbox, and its significance is unlikely to diminish. However, it is essential to recognize that while email is among the most efficient means of communication, it also presents the greatest vulnerability to cybercriminal exploitation. Also, delivery of email messages to intended recipients is often jeopardized as organizations and users enhance security measures and filtering to fend off phishing scams and spam.

In a notable action, major email providers like Google and Yahoo started rejecting emails from improperly configured services in February 2024.

Blocked emails leave no trace or notification for the sender, and because the email provider filters them, they do not appear in the recipient's junk or spam folders. This scenario underscores the delicate balance between security measures and the seamless flow of communication.[1]

Websites and Social Media Platforms. Other methods of contacting law firms include website forms and social media channels like LinkedIn, Facebook, Google Business, Snapchat, Instagram, and YouTube. Once deemed irrelevant for business purposes, these platforms have become essential for spreading the word about law firms and establishing connections, particularly with prospective clients.

Website contact forms are intricate systems with numerous components, including an email feature that may be subject to blocking. Regularly testing and reviewing these forms is vital to confirm that they operate smoothly and that the intended recipients are receiving the emails people send via a website.

The Technical Challenges of Communicating

Implementing and adopting a new communication platform requires careful evaluation, whether the platform will be used internally with staff, externally with current and prospective clients, or both. Here are some common pitfalls when implementing new technologies.

VoIP. When set up correctly, VoIP phone systems can lead to improved call quality. Using equipment that prioritizes voice calls and having sufficient network bandwidth are crucial for optimal performance, as is investing in business or enterprise-grade equipment such as managed switches and routers, rigorous testing, and network optimization.

Many small firms and businesses use consumer- or home-grade networking equipment purchased from a department store. While sufficient for most internet-based activities, these devices rarely allow users to segregate and prioritize the voice traffic on their networks, resulting in poor-quality calls.

Before transitioning to a VoIP telephone system, lawyers should ensure the service provider conducts a comprehensive assessment of network traffic quality and confirms the ability of the firm's infrastructure to prioritize voice calls for superior quality. This evaluation can be performed using a noninvasive monitoring application that observes a firm's network traffic for approximately one week. The app then reports to the firm's IT provider about the existing infrastructure's ability to support voice traffic. This crucial step, which many VoIP and IT companies skip, is the proverbial "stitch in time that saves nine." Conducting this preliminary investigative work can prevent future frustrations and subpar phone call quality.

Email and Other Communication Methods. Email security presents significant challenges that necessitate a blend of technological solutions and thorough education. For instance, the "To," "Cc," and "Bcc" fields of an email, along with attachment names and subject lines, cannot be encrypted. Consequently, these headers should not contain personally identifiable information. Moreover, emails traverse the internet in clear text, like sending a postcard, making their content visible.

Integrating a third-party application or add on is essential for encrypting emails manually or automatically. This requirement has led to encrypted email services, which necessitate logging into a secure portal to view and respond to messages. This method stands as the sole strategy to guarantee privacy in email communication. However, it introduces technological complexities and a learning curve for staff and clients, so balancing security measures with usability is crucial.

Text messaging and social media communication present a significant challenge due to the limited control over their management, aside from mandating the use of specific applications or tools.

Is faxing dead? No. It is possible to use a simple adapter to connect a fax machine to a VoIP solution and continue using the fax machine. There are now e-fax solutions, often provided by VoIP providers or third parties (such as eFax), but not all of these are secure (unlike fax

machines). For example, faxes sent via email lose the benefits of secure transmission. Also, not all online fax services have built-in security and some require a subscription. As with other technology tools, it's essential to understand how the technology works before implementation. An IT partner can be invaluable in this situation.

Ensuring Security in Communications

In the past, people rarely took steps beyond firmly sealing envelope flaps. However, as communication and collaboration increasingly depend on technology, the responsibility for implementing, troubleshooting, and ensuring the security of these methods largely falls on users. As communication methods have advanced, so too have the potential risks and threats to privacy and security. Securing communications has become increasingly important because of the abundance of personal information shared online and across various platforms.

Email and text messages top my list of tools that are not secure if improperly configured and implemented. Because clients or prospective clients often prefer them and many lawyers consider them the most convenient, efficient way of communicating, it is important to consider security and privacy of these two complex forms of communication. Of course, my focus is technology, and I assume lawyers are familiar with the ethical and privacy needs. However, statistics such as the ones below demonstrate that there are significant misconceptions about email security[2]:

• 44% of people think an email is safe if it has familiar branding (if it says Microsoft and looks like Microsoft, it must be Microsoft).

• There has been a 76% increase in financial losses from phishing.

• 30 million malicious emails were sent in 2022 with Microsoft branding.

• 21% of people surveyed don't know that an email can come from someone other than the sender.

• 63% of people surveyed don't know that email link text may not match the website.

• 62% believe that internal emails are safe.

• 68% believe their company can block all malicious email.

For email protection, I recommend users evaluate solutions that include the following:

• The ability to send and receive encrypted emails (usually via a portal);

• Filtering for spam, phishing, and other threats, which keeps malicious email from reaching inboxes;

• Archiving, to capture and store for potential later availability for e-discovery all email that passes through a system; and

• Education, because participating in cybersecurity training programs adds human beings to the security mix.

As mentioned, SMS texting (from one phone to another) is unsecure and not encrypted and should never be used to discuss anything confidential. The same holds for messages received via most social media platforms. However, Facebook recently enabled end-to-end encryption by default, and in the past few months, Meta has started implementing it as a default feature across its platform.[3]

Exercise caution with other platforms. While text messaging, or SMS, lacks security and should never be deemed secure, apps with quality encryption and security features exist. For instance, Signal (https://signal.org) and Threema (https://threema.ch) are known for their high-quality end-to-end encryption services.

During a recent trip, I discovered that WhatsApp is widely used in South America and offers encrypted calls and texts. However, because Meta owns WhatsApp, I recommend conducting thorough due diligence on this and all similar services.

Lawyers who choose to use specific secure apps must enforce their use rigorously in their practices and for clients.

Although forms on websites, such as contact forms, might provide security while data is being entered, what happens with the information afterward may not be guaranteed. For example, if web form results are emailed to a law firm, they are no longer secure or encrypted. The best policy is to advise website users not to use web forms to submit confidential information.

Conclusion

In the past decade, there has been an incredible transformation in communication technology. It has been a game-changer, especially in the business world, where most people have moved from traditional emails and phone calls to a dynamic mix of social media, instant messaging apps, and cutting-edge videoconferencing.

These advancements may have made day-to-day operations smoother, opening doors to more effective ways of connecting both within and outside organizations. Yet, as much as we've benefited from these technologies, they've also introduced new challenges.

The Computer Center has a free resource center on communication, available at https://info.computer-center.com/techcommunication. **WL**

ENDNOTES

[1]Sead Fadilpašić, *Google and Yahoo Have Changed Their Policy, Here's What You Need to Know and What to Do*, TechRadar (Feb. 8, 2024), https://www.techradar.com/computing/software/google-and-yahoo-have-changed-their-policy-heres-what-you-need-to-know-and-what-to-do.

[2]Proofpoint, *2024 State of the Phish* (March 5, 2024). https://www.proofpoint.com/us/resources/threat-reports/state-of-phish.

[3]Loredana Crisan, *Launching Default End-to-End encryption on Messenger*, Meta (Dec. 11, 2023), https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/. **WL**