30 *Ethics, Security, and Other Practical Issues*

Collaboration tools take lawyers into uncharted waters in many ways. In this chapter, we discuss some of the issues that collaboration tools raise in areas of particular concern to lawyers: ethics, confidentiality, and privilege in the practice of law. Even ten years on from the first edition of this book, lawyers are still relative newcomers to using collaboration tools, so we will attempt to reason from analogies with practices and examples that already exist. If bar regulators can understand collaboration tools as evolutionary rather than revolutionary changes and as extensions of processes lawyers already use and know well, they may decide that new types of regulation are not necessary. However, if bar regulators treat these tools as presenting completely new issues requiring completely different approaches, we all could be in for a wild ride.

Lawyers have not yet systematically addressed the ethical and related issues raised by the use of email, the Internet, data storage, and computer technology in general. ABA Formal Opinion 99-413, which states that unencrypted email between lawyer and client does not lose its confidential nature, has been accepted as approving the nonuse of encryption for routine email. However, Formal Opinion 477, issued in 2017, recognizes that some circumstances *do* warrant the use of "particularly strong protective measures," including encryption. Because Formal Opinion 477 is not limited to email but to all lawyer communications, lawyers would be well-advised to review it prior to implementing any type of technology, including the collaboration tools we mention in this book.

Unfortunately, if you search through the applicable ethical rules and comments you will not find any references to Slack, service-level agreements, cloud computing, or strong passwords. Although ethics opinions have started to address technology outsourcing, cloud services, and collaboration tools like Google Docs and Office 365, technology continues to change at a rapid pace while ethics opinions lag behind. As a result, when dealing with the ethical issues involved with collaboration tools, you should work from a clear understanding of basic legal ethics principles, take reasonable steps, monitor developments, and look to the technology itself for answers.

In the past, ethical questions involving the use of technology tended to arise and be addressed in the context of marketing, especially on the Internet. Lately, attention is being paid to the area of electronic discovery, particularly the use of metadata. We have also seen activity, largely driven by malpractice insurance carriers and state bar practice management advisors, in the areas of conflict checking, case management, and billing and accounting. Collaboration tools, especially those found online, can raise similar questions. We have seen some ethical guidance on social media and metadata, but not a lot of clarity.

In this chapter, we want to discuss other areas where collaboration tools inevitably will have a large impact: confidentiality, lawyer-client privilege, and what it means to represent a client in the Internet era. Collaboration tools raise difficult issues, but they also often contain the means to address them. If reasonable practices and procedures will be the solution to these problems, how can we start to determine what is reasonable?

Confidentiality and Security

Confidences are easy to keep when few people have access to the information. They are easy to manage when they exist within a physical document that can be locked away in a safe deposit box. Once information is stored in digital form, it becomes easy to copy and move, and much more difficult to secure, especially when it is stored on or accessible via the Internet.

A 2012 amendment to Model Rule 1.6 (Confidentiality of Information) in the Model Rules of Professional Conduct makes it explicit that attorneys must make reasonable efforts to protect against inadvertent disclosure and unauthorized access to information relating to clients. Amendments to the comments provide for a risk based analysis for confidentiality in attorneys' use of technology and electronic communications.

It's a fact that the game today is drastically different from when we dealt only with paper. We are not likely to go backward. If you use collaboration technologies in your practice, especially tools that potentially

expose your data to outside parties by means of the Internet, you must consider the impact on your ethical obligations of confidentiality. At the same time, this obligation must be interpreted within the context of the real world of computer security.

Over the years, terms like hacking, cracking, and phishing have entered our lexicon, along with social engineering, spoofing, and identity theft. Microsoft and other software vendors routinely release patches for security flaws that would permit someone to access and control a computer. Ransomware, keystroke loggers, Trojan horses, and other malware create a perilous environment for any computer connected to the Internet, even with appropriate protection. Outsiders can access unsecure wireless networks, and packet sniffers, password crackers, and hacking toolkits comprise the arsenal of today's wrongdoer, increasingly a professional data thief, mysterious government actor, or someone involved in organized crime. Computer security is an ongoing chore and a never-ending battle.

Security is the technology analogue of confidentiality. To be successful and ensure your collaboration tool gets used, the security around the tool must involve a balancing between protection and convenience. To protect something perfectly will all but guarantee that it will be inaccessible and unusable to the collaborator. Consider cartoons where characters lock the door and throw away the key. If your collaboration tools are behind that door, they aren't of much use to you. On the other hand, maximizing user convenience and access (no passwords or other barriers) effectively will eliminate any protection of the data. Security, and therefore confidentiality, requires finding the right balance.

Security requires a multifaceted approach. Authentication (including multi-factor authentication), authorization, encryption, and other security technologies all play a key role. You also will need to augment these security features with procedures and processes designed to maintain security, which would include not only firm-based procedures but also address the personal dimension of security: strong passwords, user training, and good practices.

As we discussed in Chapter 17, the security of most collaboration tools combines some level of authentication and authorization. You need to be certain the person using the tool is actually the person with permission to do so; this is the authentication component, with usernames and passwords its primary tools. Once someone is authenticated, their access and rights must be limited to only those areas to which they are actually allowed. Users are walled off from data they do not have permission to see, and they are not allowed to access, copy, or change data for which they have no permission. That is where authorization comes into play. It is usually handled by setting network permissions, designating user rights, and placing certain users into groups with defined roles.

Identity management combines authentication and authorization into one seamless process. Once the system verifies your identity, your rights adjust automatically as you move within a tool or from one tool to another. Because lawyers and others work on many different matters and may have different roles in each of those matters, identity management can invisibly tailor a user's experience so they can access and work on all of their matters, without requiring multiple logins or other annoying procedures. These security measures will help you manage confidential information, maintain ethical boundaries, and log and track access to materials.

It is also important to ensure your online activities are secure. The most common standard for securing a website involves the use of the Secure Sockets Layer (SSL)/Transport Layer Security (TLS). You'll know you're visiting a site with SSL/TLS when the URL starts with an https:// rather than an http://. Sites with SSL/TLS security should be a requirement for your online collaboration tools, whether you host them or use someone else's service. Online collaboration tools also often use encryption during transmittal of data. As use of collaboration tools increases, expect all forms of encryption to become more common, including the use of digital certificates.

Finally, your security scenario should have an emphasis on strong passwords and multi-factor authentication. Because longer, complex passwords are harder to crack, a strong password consists of combinations of letters (upper and lower case), numbers, and symbols (for example, b5@2057*JMS). The longer your password the better. The current advice is to use long passphrases that you can remember or use a password manager to generate long random passwords. Some online tools show you the strength of your password when you register, and encourage you to create stronger passwords. Your organization can also enhance security by enforcing strong password requirements. Some organizations use randomly generated passwords created by a fob or token—a small hardware device that is synchronized with a network's password on a minute-by-minute basis. This approach is a good illustration of multi-factor authentication. That means a combination of something you know (password), something you have (fob or smartphone), or something you are (fingerprint, retina scan, voiceprint, or face identification).

Biometric forms of "passwords," like fingerprint or even retina scanners, might also come into wider use, partly because of people's tendency to use weak passwords. Each year, security companies conduct surveys that show that the most commonly used password is something like "123456," "password," or "password1," which only reinforces the need for greater security measures. Some authentication will use location or past behaviors as an additional layer of authentication.

Privilege

Some feel the attorney-client privilege is under attack in the United States. That view may be open for debate, but it is fair to say that the privilege seems to be shrinking and its limits are harder to discern. Use of collaboration tools may only add to the confusion regarding the scope of the attorney-client privilege, but such tools do have the potential to help.

Collaboration tools allow lawyers to tag or label privileged material and protect it electronically, limiting access, tracking use, and providing ways to validate that the material was properly handled. For example, on a litigation extranet, privileged material can be segregated to a certain area of the site, with access tightly controlled. Comments, labels, tags, and access mechanisms can all help in identifying and working with this material.

A related issue is the inadvertent waiver of privilege. Lawyers' use of technology is fraught with danger and risk, and not just in the area of collaboration tools. Consultants and vendors increasingly have unrestricted access to our computer systems. Further, various types of IT services, hosting, and even license agreements may contain provisions allowing third-party access to data, which can raise privilege and confidentiality issues. Lawyers must pay close attention to these agreements and adequately address any specific concerns they may have.

Other Practical Issues to Watch For

As lawyers use hosted collaboration services more and more often, they will need to keep a watchful eye on potential security issues that arise in the cloud or other hosted environments. Security, disaster recovery, backup, archiving, and redundancy are among the big concerns. Other important issues include loss of data, support levels, response times, warranties, limits on liability, error handling, uptime, and bandwidth requirements. In addition, if you experience problems with your online tools, you will want to have clearly defined escalation procedures, termination and other exit strategies, and requirements for the safe return of your documents and data in a timely manner. You'll also want to formulate procedures for easing transition to a replacement provider if moving to a new service becomes necessary. Software licenses and hosting agreements in the IT industry are notoriously one-sided in favor of vendors, so you cannot expect the "standard contract" to be adequate. It's important to note that many of the same issues arise when lawyers host tools on their own computers.

Further, because some online collaboration tools, especially social media, offer a communications channel to non-clients, you run the risk that communications to these individuals may run afoul of your state's advertising and solicitation rules. These rules might affect what you can say online and whether you need to retain your online materials, apply for preapproval, or comply with other rules that typically apply to advertising or communications directed to non-clients on the Internet.

We've only looked at the tip of the iceberg on practical security issues that might arise when developing a collaboration strategy. Many other questions remain. How do electronic discovery rules apply to documents stored in collaboration tools? Will you be obligated to produce materials held in document repositories? How will the question about handling metadata be resolved? What are a lawyer's obligations for maintaining data in online tools after the project or matter is completed? What happens when vendors offering hosted sites go out of business or lose data? Who is responsible if payments for online services are not made, and the service is suspended?

You'll also have to deal with maintenance and supervision issues whether you host your collaboration tools internally or use a third-party provider. Who sets and manages user access and permissions? How are updates handled? Who fixes broken links? How long are you required to keep a collaboration site active after the project or matter is completed? And what if clients or lawyers switch firms—how do you transfer the data in your tools to them? We expect the answers to these questions will develop in the coming years.

Last but certainly not least, we must now consider Comment 8 to Rule 1.1 (Competence) of the Model Rules of Professional Conduct, which twenty-eight states have adopted as of this writing. It states:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant* technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. [emphasis added]

Our book is an argument that collaboration tools are indeed a relevant technology, and that lawyers who use collaboration tools in their practice have an obligation to understand both the risks and benefits of using such technologies.

All of these practical issues are manageable, especially if you think about them and plan for them in advance. Your best approach is to treat collaboration tools as something you will be using over the long haul and to start addressing these issues from the outset. You will also need to monitor developments constantly and watch for advice from malpractice carriers as well as opinions and rule changes from bar regulators. With careful planning, you'll be able to navigate the uncharted waters of collaboration tools with greater confidence.