To improve your writing, revisit some basics

By Matthew R. Salzwedel

Good legal writing requires basic knowledge of language, grammar and usage — the opportunity to apply that knowledge logically and rhetorically; and, most importantly, repetition in mastery. Try to take a look at five simple tips to improve your legal writing, and various legal-writing authorities that support them. Next time you make a first-time appearance with a client, you will want to consider what requirements might be imposed upon an attorney when using cloud computing for the storage of client file information.

When an initial matter, an attorney may have at least a base-level comprehension of the technology and the implications of its use. While no attorney is required to know precisely how cutting-edge technology truly works or be a computer genius, the competent attorney requirements under the Rules necessitate at least a cursory understanding of any technology used for the representation. As the preservation of the confidentiality of client information is paramount importance to the attorney-client relationship, an attorney must be aware of the potential risks inherent in the use of cloud storage services before uploading client data to third-party-owned and operated off-site servers. Are such services secure? The short answer is the classic attorney response: It depends. No matter how good a third-party’s security system is, it is a near-requirement that anyone with enough time, money and expertise can find a way to bypass it. That truism applies equally to an attorney’s personal computer; however, the risk of a security breach of a cloud storage server is that a client’s stored information can be accessed and/or destroyed in its entirety in moments. One relatively easy and initial step an attorney can take to increase the security of client information — be it stored on- or off-site — is to keep such information password-protected. While complete security is never achievable, a prudent attorney will employ reasonable precautions and thoroughly research a cloud storage vendor’s security measures and track record before using the service. Reasonable precautions may also require an attorney to read and understand a vendor’s user and/or license agreement(s) before uploading client information to their servers. Does the vendor agreement address confidentiality? If not, is the vendor willing to sign a confidentiality agreement or otherwise bind its agents to your obligations? What happens to stored information in the event the vendor goes out of business or attorney decides to terminate use of the service? If an attorney defaults on payments to a cloud storage vendor, will the attorney still be able to access and retrieve stored client information, or will the vendor revoke the attorney’s access to the information and effectively hold the data hostage in lieu of payment? Are a vendor’s servers located in countries with less-stringent legal protections against search and seizure?

Even if the servers are located domestically, to what lengths will a vendor go tofight the subpoena of information maintained on its servers? The answers to all these questions and more need to be considered before an attorney’s utilization of cloud storage services. Despite the potential legal issues, try not to regard these as genuine headaches. You’ll find it teeming in mediocre writing. And you’ll search in vain for the simple, no other reason than to enhance your legal writing. 

In conclusion, the use of technologies such as cloud computing can be of great advantage to an attorney’s law practice and is completely acceptable under the Rules of Professional Conduct provided an attorney first conducts the requisite due diligence necessary to safeguard the integrity of stored client information.

To improve your writing, revisit some basics

By Matthew R. Salzwedel

Good legal writing requires basic knowledge of language, grammar and usage — the opportunity to apply that knowledge logically and rhetorically; and, most importantly, repetition in mastery. Try to take a look at five simple tips to improve your legal writing, and various legal-writing authorities that support them. Next time you make a first-time appearance with a client, you will want to consider what requirements might be imposed upon an attorney when using cloud computing for the storage of client file information.

When an initial matter, an attorney may have at least a base-level comprehension of the technology and the implications of its use. While no attorney is required to know precisely how cutting-edge technology truly works or be a computer genius, the competent attorney requirements under the Rules necessitate at least a cursory understanding of any technology used for the representation. As the preservation of the confidentiality of client information is paramount importance to the attorney-client relationship, an attorney must be aware of the potential risks inherent in the use of cloud storage services before uploading client data to third-party-owned and operated off-site servers. Are such services secure? The short answer is the classic attorney response: It depends. No matter how good a third-party’s security system is, it is a near-requirement that anyone with enough time, money and expertise can find a way to bypass it. That truism applies equally to an attorney’s personal computer; however, the risk of a security breach of a cloud storage server is that a client’s stored information can be accessed and/or destroyed in its entirety in moments. One relatively easy and initial step an attorney can take to increase the security of client information — be it stored on- or off-site — is to keep such information password-protected. While complete security is never achievable, a prudent attorney will employ reasonable precautions and thoroughly research a cloud storage vendor’s security measures and track record before using the service. Reasonable precautions may also require an attorney to read and understand a vendor’s user and/or license agreement(s) before uploading client information to their servers. Does the vendor agreement address confidentiality? If not, is the vendor willing to sign a confidentiality agreement or otherwise bind its agents to your obligations? What happens to stored information in the event the vendor goes out of business or attorney decides to terminate use of the service? If an attorney defaults on payments to a cloud storage vendor, will the attorney still be able to access and retrieve stored client information, or will the vendor revoke the attorney’s access to the information and effectively hold the data hostage in lieu of payment? Are a vendor’s servers located in countries with less-stringent legal protections against search and seizure?

Even if the servers are located domestically, to what lengths will a vendor go to fight the subpoena of information maintained on its servers? The answers to all these questions and more need to be considered before an attorney’s utilization of cloud storage services. Despite the potential legal issues, try not to regard these as genuine headaches. You’ll find it teeming in mediocre legal writing. And you’ll search in vain for the simple, no other reason than to enhance your legal writing. 

In conclusion, the use of technologies such as cloud computing can be of great advantage to an attorney’s law practice and is completely acceptable under the Rules of Professional Conduct provided an attorney first conducts the requisite due diligence necessary to safeguard the integrity of stored client information.

To improve your writing, revisit some basics

By Matthew R. Salzwedel

Good legal writing requires basic knowledge of language, grammar and usage — the opportunity to apply that knowledge logically and rhetorically; and, most importantly, repetition in mastery. Try to take a look at five simple tips to improve your legal writing, and various legal-writing authorities that support them. Next time you make a first-time appearance with a client, you will want to consider what requirements might be imposed upon an attorney when using cloud computing for the storage of client file information.

When an initial matter, an attorney may have at least a base-level comprehension of the technology and the implications of its use. While no attorney is required to know precisely how cutting-edge technology truly works or be a computer genius, the competent attorney requirements under the Rules necessitate at least a cursory understanding of any technology used for the representation. As the preservation of the confidentiality of client information is paramount importance to the attorney-client relationship, an attorney must be aware of the potential risks inherent in the use of cloud storage services before uploading client data to third-party-owned and operated off-site servers. Are such services secure? The short answer is the classic attorney response: It depends. No matter how good a third-party’s security system is, it is a near-requirement that anyone with enough time, money and expertise can find a way to bypass it. That truism applies equally to an attorney’s personal computer; however, the risk of a security breach of a cloud storage server is that a client’s stored information can be accessed and/or destroyed in its entirety in moments. One relatively easy and initial step an attorney can take to increase the security of client information — be it stored on- or off-site — is to keep such information password-protected. While complete security is never achievable, a prudent attorney will employ reasonable precautions and thoroughly research a cloud storage vendor’s security measures and track record before using the service. Reasonable precautions may also require an attorney to read and understand a vendor’s user and/or license agreement(s) before uploading client information to their servers. Does the vendor agreement address confidentiality? If not, is the vendor willing to sign a confidentiality agreement or otherwise bind its agents to your obligations? What happens to stored information in the event the vendor goes out of business or attorney decides to terminate use of the service? If an attorney defaults on payments to a cloud storage vendor, will the attorney still be able to access and retrieve stored client information, or will the vendor revoke the attorney’s access to the information and effectively hold the data hostage in lieu of payment? Are a vendor’s servers located in countries with less-stringent legal protections against search and seizure?

Even if the servers are located domestically, to what lengths will a vendor go to fight the subpoena of information maintained on its servers? The answers to all these questions and more need to be considered before an attorney’s utilization of cloud storage services. Despite the potential legal issues, try not to regard these as genuine headaches. You’ll find it teeming in mediocre legal writing. And you’ll search in vain for the simple, no other reason than to enhance your legal writing. 

In conclusion, the use of technologies such as cloud computing can be of great advantage to an attorney’s law practice and is completely acceptable under the Rules of Professional Conduct provided an attorney first conducts the requisite due diligence necessary to safeguard the integrity of stored client information.