Electronic Attorney-Client Communications
By Joel R. Brandes

 The attorney-client privilege is the foundation of the attorney-client relationship. CPLR 4503 (a) (1) codifies the attorney-client privilege. It provides, in part, that “Unless the client waives the privilege, an attorney or his or her employee, or any person who obtains without the knowledge of the client evidence of a confidential communication made between the attorney or his or her employee and the client in the course of professional employment, shall not disclose, or be allowed to disclose such communication, … in any action, disciplinary trial or hearing, ….”

The attorney-client privilege applies only to confidential communications between attorneys and clients that are made for the purpose of obtaining or rendering legal advice in the course of a professional relationship (Rossi v. Blue Cross & Blue Shield of Greater N.Y*.,* 73 N.Y.2d 588, 542 N.Y.S.2d 508 (1989)). For the privilege to apply when communications are made from client to attorney,  they must be made for the purpose of obtaining legal advice and be directed to an attorney who has been consulted for that purpose. For the privilege to apply when communications are made from attorney to client, whether or not in response to a particular request, they must be made to facilitate the rendition of legal advice or services, in the course of a professional relationship (Rossi v Blue Cross and Blue Shield of Greater New York, supra). In determining whether a communication is protected by the attorney-client privilege, the critical inquiry is whether, viewing the lawyer's communication in its full content and context, it was made in order to render legal advice or services to the client. In that regard, the attorney-client privilege protects communications between an attorney and his or her client that convey facts relevant to a legal issue under consideration, even if the information contained in the communication is not privileged. (Gilbert v Office of the Governor, 70 A.D.3d 1404, 96 N.Y.S.3d 724 (3 Dept., 2019)).

No attorney-client privilege arises unless an attorney-client relationship has been established. An attorney-client relationship arises only when one contacts an attorney in his capacity as an attorney for the purpose of obtaining legal advice or services. In order to make a valid claim of privilege, it must be shown that the information sought to be protected from disclosure was a “confidential communication” made to the attorney for the purpose of obtaining legal advice or services. The burden of proving each element of the privilege rests upon the party asserting it. (Priest v Hennessy, 51 N.Y.2d 62, 431 N.Y.S.2d 511, 514 (1980)).

 CPLR 4548 extends the attorney-client privilege to electronic communications such as email, text messages, and instant messages. It provides that no communication privileged under article 45 of the Civil Practice Law and Rules shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication.

The purpose of CPLR 4548 was to recognize the widespread commercial use of e-mail. The holder of the privilege and his or her attorney must protect the privileged communication from disclosure. If not, the privilege will be waived. For example, when a spouse sends her spouse a confidential e-mail from her workplace with a business associate looking over her shoulder as she types, the privilege does not attach. ( Scott v Beth Israel Medical Center Inc., 17 Misc. 3d 934, 847 N.Y.S.2d 436, 440 (Sup Ct, 2007)).

Reasonable expectation of confidentiality at home

In Willis v. Willis, (79 A.D.3d 1029, 914 N.Y.S.2d 243 (2d Dep't 2010)) the Appellate Division held that the plaintiff failed to meet her burden of demonstrating that the e-mail communications between herself and her attorneys were made in confidence where she knew the password to the e-mail account that she used to communicate with her attorneys was known to her children who regularly used the e-mail account. There was no evidence that she requested that the children keep the communications confidential. Under these circumstances, it could not be said that the plaintiff had “a reasonable expectation of confidentiality” in the e-mail communications between herself and her attorneys.

However, in Parnes v. Parnes, (80 A.D.3d 948, 915 N.Y.S.2d 345 (3d Dep't 2011)) the Appellate Division held that the defendant did not waive the attorney-client privilege for e-mails with his counsel stored in his computer even though he left a note on his desk with the username and password. The plaintiff averred that she discovered a single printed page of a five-page e-mail on a desk in the marital residence. The parties acknowledge that this desk was located in a room used as an office and the parties, their nanny, and babysitters all used that room. Defendant contended that the desk contained only his papers and the plaintiff had her desk in the same room, but the plaintiff appeared to disagree. Regardless of whether the parties had separate desks, by leaving a hard copy of part of a document on the desk in a room used by multiple people, the defendant failed to prove that he took reasonable steps to maintain the confidentiality of that page. Thus, the defendant waived the privilege as to that one page, and the plaintiff could use that single page in litigation. On the other hand, the defendant took reasonable steps to keep the e-mails on his computer confidential. Defendant set up a new e-mail account and only checked it from his workplace computer. Leaving a note containing his user name and password on the desk in the parties' common office in the shared home was careless, but it did not constitute a waiver of the privilege. Defendant still maintained a reasonable expectation that no one would find the note and enter that information into the computer in a deliberate attempt to open, read and print his password-protected documents. His wife admitted that after she found one page left on his desk, she searched through the defendant's papers in an effort to find the rest of the document, instead found the note with his user name and password, then purposely used the password to gain access to defendant's private e-mail account, without his permission, to uncover the remainder of the e-mail. Under the circumstances, the defendant did not waive the privilege as to the e-mails in his private e-mail account because he took reasonable steps to keep the e-mails on his computer confidential.

Reasonable expectation of confidentiality at work

The First Department has utilized a four-factor test to ascertain if an employee has a reasonable expectation of privacy when he uses a computer at his place of employment to communicate with his attorney.

In Peerenboom v. Marvel Entertainment, LLC, (148 A.D.3d 531, 50 N.Y.S.3d 49 (1st Dep't 2017)) the Appellate Division applied four factors to determine that the employee lacked any reasonable expectation of privacy in his personal use of the email system of Marvel, his employer, and correspondingly lacked the reasonable assurance of confidentiality that is an essential element of the attorney-client privilege. Those factors are: (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?  It observed that while Marvel's email policies during the relevant periods permitted “receiving e-mail from a family member, friend, or other non-business purpose entity . . . as a courtesy,” the company asserted that it “owned” all emails on its system and that the emails were “subject to all Company rules, policies, and conduct statements.” Marvel “reserve[d] the right to audit networks and systems on a periodic basis to ensure [employees'] compliance” with its email policies. It also “reserve[d] the right to access, review, copy and delete any messages or content,” and “to disclose such messages to any party (inside or outside the Company).” Given, among other factors, the employee's status as Marvel's Chair, he was, if not actually aware of Marvel's email policy, constructively on notice of its contents.

It has been held that an employee has no reasonable expectation of privacy regarding attorney-client communications where an employee uses a company computer to communicate with his attorney and the company handbook notifies its employees of its unlimited right of access to its computers. (See Miller v. Zara USA, Inc., 151 A.D.3d 462, 56 N.Y.S.3d 302 (1st Dep't 2017)).

Misdirected email communications

The attorney-client privilege may also be destroyed when a misdirected email is sent to your adversary by mistake. Rule 4,4(b) of the New York Rules of Professional Conduct provides that a "lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender." According to New York City Bar Association, Formal Opinion 2012-1, a lawyer who receives such a document must promptly notify the sender (in addition to identifying and following applicable substantive law) but has no other obligations under the New York Rules of Professional Conduct with respect to the retention, return, destruction, review or use of the document or its contents. Rule 4.4(b) provides the only governing ethical rule on this topic (other than the normal duty of truthfulness set forth in Rules 4.1 and 8.4).

Authentication of non-privileged communications

Emails and text messages between an attorney and her client which are not confidential communications, or protected by some other privilege, are admissible in evidence if they are authenticated. They are admissible if the proponent of an email or text message demonstrates its genuineness by clear and convincing evidence, thus laying a foundation for its admission. An email or text message must be authenticated by showing that the item sought to be introduced is what its proponent claims it to be. Emails and text messages are subject to the same rules of authentication as all other evidence.

Some text messages may be self-authenticating such as where the content of the messages makes no sense unless they were sent by the defendant. (People v Pierre, 41 AD3d 289, 838 N.Y.S.2d 546 (1st Dept.,2007)). In People v. Green, (107 AD3d 915, 107 A.D.3d 915, 967 N.Y.S.2d 753 (2nd Dept. 2013)) the Appellate Divison held that the text messages from the defendant to the complainant were properly admitted into evidence. Since the content of the text messages “made no sense unless [they were] sent by the defendant” the text messages themselves were sufficient to authenticate that they were sent by the defendant. As to the authenticity of the photographs of the text messages, the complainant's testimony that they were, “actual photographs of the screen of [her] telephone,” and that she saw the detective taking the photographs, was sufficient to establish “that the [text messages had] been accurately and fairly reproduced,” thereby providing a foundation for admission of the photographs.

Text messages have been authenticated based solely on the testimony of the owner of the phone. InPeople v Agudelo (96 AD3d 611, 947 N.Y.S.2d 96 (1st Dept., 2012)) a printout of text messages taken from the victim's phone was authenticated by the testimony of the victim that the printout accurately represented the exchange of messages. In People v. Cotto, (164 A.D.3d 826, 79 N.Y.S.3d 535 (2d Dept. 2018)) photographs of text messages between the defendant and the complainant were properly admitted into evidence where the complainant's testimony that the photographs of the text messages fairly and accurately depicted the text message conversation between her and the defendant was sufficient to authenticate the photographs.

Text messages have also been authenticated by circumstantial evidence. In People v. Washington (179 A.D.3d 522, 116 N.Y.S.3d 263 (1st Dep't 2020) the Appellate Divison held that the court providently exercised its discretion in admitting in evidence a series of text messages exchanged between a person purporting to be defendant's mother and the victim two days after the crime. There was sufficient authentication because an extensive chain of circumstantial evidence left no doubt that the texts came from the defendant. Among other things, these intimidating texts, which contained damaging admissions, reached the victim at a disguised phone number that she had shared with the defendant shortly after the crime, but had not shared with anyone else. The texts revealed a detailed knowledge of the incident and the relationship between the defendant and the victim, and they explicitly discussed the sexual encounter. The sender admitted having the victim's car, bag and phone, which were taken during the incident, and the defendant was apprehended a day later driving the victim's car. Viewed as a whole, and not as individual fragments, the circumstantial evidence made it highly improbable that anyone other than the defendant sent the texts. In addition, the sender's phone number was registered to a former female friend of the defendant.

Photographs and screenshots of text messages sometimes require a two-person authentication. In People v. Hughes (114 AD3d 1021, 981 N.Y.S.2d 158 (3rd Dept. 2014)) photographs of text messages sent from the defendant's cell phone to the victim were properly authenticated where the People produced testimony from a Verizon employee confirming that text messages had been sent between certain phone numbers, the victim identified the phone numbers as belonging to her and defendant, and she identified the photographs as depicting text messages she received from him.

 Recently, the Court of Appeals held that the trial court did not abuse its discretion in determining that the screenshots of text messages were properly authenticated and admissible in evidence based upon the testimony of a participant in and witness to the conversations with the defendant. In People v Rodriguez, (38 N.Y.3d 151, 169 N.Y.S.3d 910 (2022)) text messages that the defendant sent to the victim came to light when the victim's 16-year-old boyfriend observed them on her phone, took screenshots of messages that were sexual in nature, and forwarded the screenshots to the victim's mother and himself. The Court of Appeals held that the trial court acted within its discretion in determining that the People properly authenticated the screenshots. Here, the testimony of the victim, a participant in the conversations with the defendant, sufficed to authenticate the screenshots. She testified that all of the screenshots offered by the People fairly and accurately represented text messages sent to and from the defendant's phone. The boyfriend also identified the screenshots as the same ones he took from the victim's phone. Telephone records of the call detail information for defendant's subscriber number corroborated that defendant sent the victim numerous text messages during the relevant time period.

 Conclusion

Email, text messages and other electronic communications between an attorney and her client which do not qualify as confidential communications and are not protected by some other privilege are admissible in evidence if they are authenticated. Care should be taken when an attorney and client communicate electronically with one another because the attorney-client privilege can be destroyed where there is no reasonable expectation of privacy.

**Joel R. Brandes practices matrimonial law in New York City concentrating on appeals. He is the author of a new twelve-volume treatise, Law and the Family New York, 2022- 2023 Edition, and Law and the Family New York Forms, 2022 Edition (five volumes), both published by Thomson Reuters, and the New York Matrimonial Trial Handbook (Bookbaby). He can be reached at joel@nysdivorce.com or at his website at www.nysdivorce.com.**