Reprinted with permission from New York State Bar Association Journal, Vol. 91, No. 7| September 2019

The Attorney Professionalism Committee invites our readers to send in comments or alternate views to the responses printed below, as well as additional hypothetical fact patterns or scenarios to be considered for future columns. **Send your comments or questions to: NYSBA, One Elk Street, Albany, NY 12207, Attn: Attorney Professionalism Forum, or by email to journal@nysba.org.**

This column is made possible through the efforts of the NYSBA's Committee on Attorney Professionalism. Fact patterns, names, characters and locations presented in this column are fictitious, and any resemblance to actual events or to actual persons, living or dead, is entirely coincidental. These columns are intended to stimulate thought and discussion on the subject of attorney professionalism. The views expressed are those of the authors, and not those of the Attorney Professionalism Committee or the NYSBA. They are not official opinions on ethical or professional matters, nor should they be cited as such.

DEAR FORUM:

I am an attorney practicing civil and criminal law here in New York. I have been approached by my millennial client who is employed by a large bank. She suspects, but is not sure, that her employer, in conjunction with government authorities, is conducting an investigation of her and others in her division for potential violations of banking laws. In an effort to prepare for the defense of my client who may be facing both civil and criminal exposure, I have asked her to try and obtain information regarding the full scope of the investigation. Naturally, I have advised her to avoid creating any "paper trail" of her efforts and so have instructed her to stick to just spoken conversations with her various professional colleagues in an effort to "see what they know and have heard."

My client suggested that she could also communicate using a message app that would auto self-delete the text as soon as it is read by the recipient. I never heard of such a thing but my client showed me one of these apps and it worked great. I am concerned that one might say that using such an app intentionally is a way to destroy evidence. However, it would seem to me that such an app is just like spoken communication, unless it's recorded, leaving no record other than the parties' recollections. Please give me some guidance.

Sincerely,
Teki Challenged

DEAR MR. CHALLENGED:

It seems that you are concerned about potential criminal or civil liability if your client's investigation efforts are obtained by her employer or governmental investigators, and we are certain that is something many lawyers are concerned about. While you've not heard of such apps before, they are becoming more and more common – Snapchat, Wickr, Telegram, Confide and Gmail Snapmail all allow users to create messages that will self-destruct within a certain period of time after they are opened. The younger generation views such apps as the older generation views a phone call; after the phone call, the conversation vanishes into the ether, whereas after the app message is typed out, and read, it too vanishes into the ether, after a time predetermined by the sender of the message – 60 seconds, five minutes, a day, or after the app is closed. Some apps can notify the sender if the recipient takes a screenshot of the communication; others block the recipient's ability to even take a screenshot.

It is a close question whether such inquiry even implicates ethics rules, other than the duty, under New York Rule of Professional Conduct ("Rule") 1.1, to give competent legal advice. If it is a binary issue – either it is legal to use self-destructing messaging apps or it is not – then the attorney discharges his duty by simply advising the client that it is legal under the circumstances, or that it is not. However, having been consulted by a client for legal advice, it is incumbent upon the attorney to inquire why she seeks such advice, so that the attorney can competently advise her whether it is lawful to use such apps. After obtaining that information, there may be a clear yes/no answer, or it may no longer be a binary issue. Additionally, Rules 3.4 ("Fairness to Opposing Party and Counsel") and 8.4(d) ("Conduct Prejudicial to the Administration of Justice") may be implicated.

Certain regulated industries make the use of such apps flatly illegal. For example, banking, publicly traded companies, federal contractors, etc. are all subject to rules requiring the retention of documents, including, of course, electronic communications. (*See, e.g.*, 18 U.S.C. § 1519, 17 CFR § 240.17a-4(b)(4), and 17 CFR Part 210 of Sarbanes-Oxley regs.). Executive branch employees may not use ephemeral communications. (*See* National Archives and Records Administration Act, 44 U.S.C. 2101 et seq.) Of course, that would only apply to the business of that industry – there is no rational, logical reason that would preclude an employee in that industry from using her own smart phone with such an app to make dinner plans with a work colleague.

Documents related to hiring, evaluation, training, safety, complaints, procedures, retention, and immigration status of employees must be preserved, in order to deter or prevent discrimination and promote workplace safety. Thus, using such apps to discuss potential employees, or to communicate with references, is illegal. (*See* Civil Rights Act of 1964; Executive Order of 1965, No. 11246; Immigration Reform and Control Act of 1986).

In addition, the failure to preserve such records may, in the event of litigation, result in a missing document charge or, worse, a striking of the party's pleading. Accordingly, advising your client that she may use such apps when she is engaged in litigation or when litigation is reasonably likely, would implicate Rule 3.4, which provides that a lawyer shall not "(a)(1) suppress any evidence that the lawyer or the client has a legal obligation to reveal or produce . . . [nor] (3) conceal or knowingly fail to disclose that which the lawyer is required by law to reveal." If the proposed communications are the subject of current or reasonably anticipated litigation, the client should, at a minimum, be advised to only discuss those issues with her counsel, as there is no way to assure that such communications will truly remain secret; her counterparty may be subpoenaed to testify about the communications or may find a workaround to save the communication by notetaking or using another device to photograph the communication. And she should be advised of the risks of a missing document charge or the striking of pleadings if she nonetheless engages in such communications.

Moreover, advising her to use such apps when engaged in litigation, or when litigation is reasonably anticipated, may implicate Rule 8.4(d), as it may be deemed to be conduct prejudicial to the administration of justice. "A lawyer or law firm shall not … engage in conduct that is prejudicial to the administration of justice."

In *Waymo v. Uber*, U.S. Dist. Ct., Northern Dist. of Cal., Docket No. 17-cv-00939, discovery sanctions were issued against Uber, whose executives used the self-destructing message apps Wickr, Telegram and Signal to communicate. Uber had hired an executive away from Google's Waymo subsidiary, which had been created to develop self-driving cars. Litigation ensued, in which Waymo accused Uber of stealing its trade secrets. In an order dated January 29, 2018 (Docket Entry 2585), Federal Judge Alsup held that an adverse inference could be drawn against Uber at trial for its use of such messaging apps, and failure

to preserve the messages sent and received using those apps. "Uber's use of ephemeral messaging may be used to explain gaps in Waymo's proof that Uber misappropriated trade secrets or to supply proof that is part of the res gestae of the case (like the due diligence report)." (*Id.* at 5). Moreover, at a bench hearing, Federal Judge William Alsup stated that attorneys who fail to turn over evidence of such communications may be found to have committed legal malpractice. (*See* Paresh Dave & Heather Somerville, *Uber's Use of Encrypted Messaging May Set Legal Precedents*, Reuters, Nov. 29, 2017).

As a *general* proposition, it would be unwise, if not unethical, to advise anyone working in any of these sectors – publicly traded companies, financial institutions, governmental employees, health and safety communications, and the like – that it is acceptable to communicate using self-destructing emails regarding the business of such sectors. To be sure, an attorney should absolutely advise the client against using such communications where it is known that their revelation would be germane to litigation. As a matter of best practices for e-discovery preservation, once on reasonable notice of potential litigation, an attorney should advise their client to disable the automatic deletion of ephemeral communication and institute a "litigation hold." Thomas J. Kelly & Jason R. Baron, *The Rise of Ephemeral Messaging Apps in the Business World*, The National Law Review, April 23, 2019, citing The Sedona Conference Commentary on Legal Holds, Second Edition: The Trigger & The Process (Public Comment Version, Dec. 2018), *available at* https://thesedonaconference.org/publications.

During discovery, it is now routine for parties to inquire about the use of such apps, and, while the messages may no longer exist, the mere fact of the use of these apps may be used to paint a picture of furtiveness intended to hide the truth.

But is that always the case? What if the client is a whistleblower, who has information regarding illegal conduct on the part of her company or governmental agency? First, we note that regardless of any confidentiality agreement or non-disclosure agreement, there is no societal interest that protects against the disclosure of criminal conduct (save for the societal interest in permitting those who have committed crimes to speak with their counsel, etc.), and thus such confidentiality and non-disclosure agreements are void, to the extent that they purport to bar such disclosure. (*See* 7 Williston Contracts §15:8.)

Second, we note that it is well established that information regarding criminal activities cannot be considered "confidential," save for the traditional sense that a client's privileged communications with her attorney (or her spouse, clergyman or doctor for that matter) about a past crime are privileged. If the whistleblower has information that her company or governmental agency has broken or is breaking the law, it is simply not "confidential" information; she may freely disclose it. See *Restatement (Third) Agency* § 8.05, *comment c*: "[A]n agent may reveal to law-enforcement authorities that the principal is committing or is about to commit a crime. An agent's privilege to reveal such information also protects the agent's revelation to a private party who is being or will be harmed by the principal's illegal conduct." As crime, by definition, harms the public generally, the principle stated in the *Restatement* is arguably too narrow for our democratic system: If a crime has been committed or is being committed, it is the public that is harmed, not just a private individual. So what if the client wishes to communicate anonymously, through the Fourth Estate, the media, about illegal conduct of a company or governmental agency? Is it ethical to advise the client – who does not wish her identity to become known for risk of retaliation – to use ephemeral messaging apps to communicate with the media to get the story out? As the communications are legal, it is thus ethical to advise the client to communicate using ephemeral messaging apps.

And what if the client has brought or is contemplating bringing a discrimination lawsuit against her employer? Would it be appropriate to advise her that she may communicate with her co-workers using ephemeral messaging apps in order to gather evidence? Attorneys always ask their clients to provide them with evidence to support their claims. The use of ephemeral messaging apps, however, subjects the client to the possibility that she will be accused of conspiring with co-workers to concoct a story and questioning regarding the use of such apps at deposition is becoming routine. If the client uses such apps to communicate with co-workers, it must be assumed that it will be disclosed and that she will be depicted by her adversary as duplicitous and conspiratorial in front of a jury. In accordance with Rule 1.1., the duty to provide competent counsel, the client should be advised of such risks.

Sincerely,
The Forum by

Richard E. Lerner
(richard@mazzolalindstrom.com) and
Jean-Claude Mazzola
(jeanclaude@mazzolalindstrom.com)
Mazzola Lindstrom LLP
Vincent J. Syracuse
(syracuse@thsh.com) and
Carl F. Regelmann
(regelmann@thsh.com)

Tannenbaum Helpern Syracuse & Hirschtritt LLP

QUESTION FOR THE NEXT ATTORNEY PROFESSIONALISM FORUM:

In order to attract new clients in the cryptocurrency space, I raised the prospect of accepting cryptocurrency as payment for legal fees with our firm's management committee. I think that offering clients a cryptocurrency payment option will make us more attractive to some clients that are participating in the growing cryptocurrency marketplace and help present ourselves as a technologically savvy and knowledgeable law firm.

If our firm decides to accept cryptocurrency as payment for legal fees, are there any ethical issues we should be aware of before proceeding? Are there any prohibitions on a firm accepting cryptocurrency payments? Is the payment of cryptocurrency by a client to a law firm for legal services already rendered the equivalent of a wire payment? Are there any specific requirements for holding the client's cryptocurrency in our law firm trust accounts? At some point, could we require a client to pay with cryptocurrency? Are there any other issues concerning cryptocurrency payments that we should consider?

Sincerely,
Al T. Coyne

UPDATE TO MAY 2019 FORUM ON INADVERTENT DISCLOSURE

We wanted to update you on a recent ethics opinion that was published after our May 2019 Forum on the same topic went to press (Vincent J. Syracuse, Carl F. Regelmann & Alexandra Kamenetsky Shea, Attorney Professionalism Forum, N.Y. St. B.J., May 2019, Vol. 91, No. 4). In our May 2019 Forum, we discussed an attorney's obligations when the attorney receives inadvertently produced material. (*Id.*) On May 16, 2019, the New York City Bar Association Committee on Professional and Judicial Ethics issued Formal Opinion 2019-3 on this very topic. NYCBA Comm. on Prof'l and Jud. Ethics, Op. 2019-3 (2019). The Committee opined that after notifying the sender of the inadvertently produced materials pursuant to Rule 4.4(b), and subject to any rules, agreements, or court orders to the contrary, "[i]f using the inadvertently sent information would reasonably be expected to advance the client's objectives and the law permits its use, then Rules 1.2(a) and 1.4 direct the lawyer to consult with the client about the risks and benefits of using the information. The client's desire to use the information should be treated by the lawyer as controlling when the failure to do so would constitute a failure 'to seek the objectives of the client through reasonably available means permitted by law and these Rules' under Rule 1.1(c), and/or would 'prejudice the rights of the client' under Rule 1.2(e)." (*Id.*) "[I]f the lawyer and the client have a fundamental disagreement over whether to use the inadvertently disclosed information, the lawyer may be permitted or required to withdraw from the representation depending on the circumstances." (*Id.*) As the opinion noted, there may be many reasons why an attorney would be disinclined to use the inadvertently disclosed information including a lawyer's perceived "higher professional duty." (*Id.*) Should you come across inadvertently produced materials, we recommend reading this opinion as you consider your ethical obligations.