ATTORNEY PROFESSIONALISM FORUM

Dear Forum,

I keep hearing stories of hackers breaking into the computer networks of law firms to steal confidential customer information. I am the managing partner of a 50-attorney firm and I must say this is keeping me up at night. I would appreciate some guidance on what a law firm's ethical obligations are with respect to guarding against the consequences of a cyberattack. Do we have any obligations with respect to the various vendors we hire?

Sincerely,

Sleepless in New York

Dear Sleepless in New York:

Cloud computing and the rise of mobile devices have changed the way companies of all kinds do business, including law firms. Along with these technological leaps have come a variety of cybersecurity issues affecting both lawyers and clients alike. A failure to take reasonable steps to preserve the confidentiality of client data can be more than bad business; it can lead to ethical violations and even potential liability. Attorneys have a professional obligation to maintain the confidentiality of client information (New York Rules of Professional Conduct (NYRPC 1.6(a)), and to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of that information (NYRPC 1.6(c)).

Under NYRPC 1.6, attorneys have two distinct duties to preserve the confidentiality of client information. First, NYRPC 1.6(a) prohibits attorneys from knowingly revealing a client's confidential information, or such other information that may disadvantage the client, unless: (1) the client gives informed consent (as defined in Rule 1.0(J)); (2) the disclosure is impliedly authorized to advance the client's interest and is reasonable under the circumstances; or (3) the revelation fell into one of the specified exceptions of subsection (b) (e.g., necessary to prevent a crime, bodily harm, etc.). Attorneys' second duty under NYRPC 1.6 is more ambiguous – attorneys have an obligation to "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client." This standard of reasonableness should be familiar to most practicing attorneys, but may not be especially helpful for ensuring client confidentiality in an era of cutting-edge technological evolution, where there is a limited history of what constitutes "reasonable care." Nevertheless, "the reasonable person . . . is called upon . . . when a problem arises that needs to be solved objectively," and attorneys have no choice but to grapple with their responsibilities to clients on the issue of cybersecurity. (John Gardner, *The Many Faces of the Reasonable Person*, NYU Law Review, http://www.law.nyu.edu/sites/default/files/upload_documents/The%20Many%20Faces%20of%20the%20Reasonable%20Person.pdf).

Complying with these obligations can be an increasingly daunting challenge when "new technologies create new threats to the confidentiality of client data." *See* Drew Simshaw and Stephen Wu, *Ethics and cybersecurity: Obligations to Protect Client Data*, National Symposium on Technology in Labor and Employment Law (March 15, 2015). Indeed, the security of digital data has become an issue of national significance. As FBI Director at the time Robert Mueller recognized in March 2012 "there are only two types of companies: those that have been hacked and those that will be." American Bar Association, *Cybersecurity: Ethically Protecting Your Confidential Data in a Breach-A-Day World* (April 27, 2016).

Law firms are not immune from cyberattacks. Indeed, in March of 2016, a Russian cyber-criminal targeted nearly 50 large law firms in an attempt to obtain the confidential financial information of several of their largest clients. *See* Claire Busher, *Russian Cyber Criminal Targets Elite Chicago Law Firms*, Crain's (March 29, 2016). Hackers managed to breach the computer networks of some of the world's most prestigious law firms, including Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP. *See* Nicole Hang and Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, Wall Street Journal (March 29, 2016). The FBI has warned that law firms will continue to be targeted for cyberattacks because they have access to their clients' most sensitive and valuable information, and are viewed by hackers as relatively easy targets. *See* Simshaw and Wu, *supra.*

Whatever their size, sector or location, attorneys and law firms have an ethical obligation to institute and maintain sound cybersecurity protocol, and to ensure that third-party vendors do the same. The NYRPC commentary is unambiguous – "to maintain the requisite knowledge and skill, a lawyer should . . . keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients ***or to store or transmit confidential information***." (Comment 8 to NYRPC 1.1 (emphasis

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.

added).) As commentators have recognized, "the requirement to protect client information is, in essence, an information security obligation," and the New York State Bar Association (NYSBA) and the American Bar Association (ABA) have provided attorneys with some guidance on how attorneys can go about satisfying this obligation. *See* Simshaw and Wu, *supra*.

The NYSBA Committee on Professional Ethics has issued several ethics opinions setting forth the scope of attorneys' obligations to maintain the confidentiality of clients' electronic data under the NYRPC, and what steps attorneys can take to ensure they satisfy their obligations. For instance, in September 2010, the NYSBA Committee on Professional Ethics issued Ethics Opinion No. 842, which dealt primarily with the use of outside online storage providers – commonly referred to as "cloud computing" – to store client data. Opinion No. 842 noted that the storage of client data "in the cloud" implicated NYRPC 1.6 (confidentiality of information), and dealt with an inquiry concerning a solo practitioner's use of cloud storage systems to preserve client data in the event that something was to happen to his own personal computer.

NYSBA Committee on Professional Ethics Opinion No. 842 unequivocally states that in this era of cloud computing, "[a] lawyer must take reasonable affirmative steps to guard against the risk of inadvertent disclosure by others who are working under the attorney's supervision or who have been retained by the attorney to assist in providing services to the client." In today's world, that means taking certain precautions to preserve the confidentiality of a client's digitally stored information. For example, attorneys entrusting confidential information to a third party such as a cloud service provider should ensure that: (1) the service provider has an enforceable obligation to preserve confidentiality and security; (2) the service provider employs available technology to thwart reasonably foreseeable attempts at infiltration; and (3) the lawyer periodically reviews the security protocol in place to ensure that it is still adequate and reasonably up to date. It should be noted that in the scenario presented in Opinion No. 842, the solo practitioner's online data storage system was password-protected, and the data stored on the system was encrypted. These are the types of steps that might satisfy an attorney's obligation under NYRPC 1.6(c) and which, depending upon the circumstances, may represent the bare minimum of what an attorney is required to implement in terms of technical specifications in order to satisfy his or her duty of reasonableness. However, because the nature of cybersecurity is changing rapidly, attorneys "should periodically reconfirm that the provider's security measures remain effective in light of advances in technology." Opinion No. 842.

In August 2014, the NYSBA Committee on Professional Ethics issued Ethics Opinion No. 1019, addressing issues of confidentiality arising from attorneys accessing their firm's electronic files remotely. Working remotely has become an everyday occurrence for most attorneys, who have grown accustomed to the convenience of being able to service a client's needs at a moment's notice, and from anywhere in the world with an Internet connection. However, a 2014 report by the Department of Homeland Security found that "online tools that help millions of Americans work from home may be exposing both workers and businesses to cybersecurity risks." Michael Roppolo, *Work-from-home remote access software vulnerable to hackers: Report*, CBS News (July 31, 2014). In order to access files remotely, attorneys often log on to unsecure Wi-Fi networks or "hotspots," which can expose both the attorney and the firm's files to malware – software designed by hackers that can infiltrate remote desktops and whose capabilities include logging keystrokes, uploading discovered data, updating malware and executing further malware. As the NYSBA Committee on Professional Ethics itself has acknowledged, "lawyers can no longer assume that their document systems are of no interest to cyber-crooks" and that is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system.

Unfortunately, Opinion No. 1019 provides attorneys little in the way of detail as to how they can work remotely without compromising their own ethical obligations in the process. The Opinion directs attorneys to Comment 17 to NYRPC 1.6, which provides that attorneys are not obligated to "use special security measures if the method of communication affords a reasonable expectation of privacy." "The key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure." NYRPC No. 1019, ¶ 5. However, "because of the fact-specific and evolving nature of both technology and cyber risks, [it] cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information coming into the hands of unintended recipients." (*Id.* ¶ 10.) As a result, attorneys would be wise to err on the side of caution when accessing client information remotely, and to look to other resources for technical guidance.

Fortunately, there are a number of cybersecurity resources available to attorneys that may provide further guidance on best practices. Specifically, the ABA has published a handbook to help lawyers and their firms cope with the emerging cybersecurity threat. *See* Jill D. Rhodes & Vincent Polley, *The ABA Cybersecurity Handbook*, ABA Cybersecurity Legal Taskforce (2013). In addition, on May 11, 2017, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion No. 477, which provides a non-exhaustive

list of best cybersecurity practices for attorneys. Among other things, the committee recommends that attorneys: (1) understand the nature of the cybersecurity threat, including a careful consideration of the sensitivity of a client's information and whether a particular client is at a higher risk for attack; (2) understand how the firm's electronic communications are created and stored, so that a lawyer may assess and manage the risk of inadvertent disclosure; (3) understand and use reasonable security measures, such as the use of secure internet access methods; (4) train non-lawyer support staff in the handling of confidential client information; (5) clearly and conspicuously label confidential client information as "privileged and confidential"; and (6) conduct due diligence on third-party vendors providing digital storage and communication technology. While the utility of specific security measures may vary depending upon particular circumstances, compliance with these types of practices will go a long way toward attorneys' ongoing attempts to comply with their ethical obligations while storing and using client's digital information, or when working remotely.

Moreover, the Association of Corporate Counsel, a bar association that promotes the interests of in-house counsel, has also issued a set of guidelines for outside counsel's protection of confidential client information. *See Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information*, Association of Corporate Counsel (the "ACC Model Controls"). The ACC Model Controls provide detailed recommendations for the handling of confidential client data, with a particular emphasis on encryption. Encryption is the process of converting digital information into a code, to prevent unauthorized access by outside parties. One commentator has compared sending unencrypted data over the internet to mailing a postcard without an envelope – it can be accessed and read by just about anyone. The ACC Model Controls therefore suggest the encryption of client data while in transit, as well as encryption of all information stored on outside counsel's systems, servers and mobile devices. The ACC Model Controls also mandate the reporting of any data security breach to the client within 24 hours of discovery of the breach (ACC Model Controls § 3.2).

The failure to employ basic data-security measures can have drastic consequences, including the imposition of civil liability for professional malpractice. In the wake of the data breach at Cravath, Weil Gotshal and other large firms in March 2016, a plaintiffs' law firm planned to initiate a class action lawsuit against them for their failure to preserve the confidentiality of client information. *See* Aebra Coe, *BigLaw in Crosshairs as Firm Plans Data Breach Litigation*, Law 360 (March 31, 2016). In New York, former clients filed a complaint against their attorney following a "spoofing attack" which caused them to wire nearly $2 million to hackers, instead of counsel. *See Millard v. Doran*, Index No. 153262 (Sup. Ct. N.Y. County 2016). The former clients alleged that the attorney's maintenance of her law firm email account on America Online constituted professional negligence and a breach of her fiduciary obligations in light of AOL's track record of vulnerability to hacking attacks. In another case, a client brought suit even prior to the occurrence of an actual data breach, citing the clear gaps in the firm's cybersecurity protocols. *See Jason Shore and Coinabul v. Johnson N& Bell*, Docket No. 1:16-cv-or04363 (N.D. Ill. April 15, 2016).

In addition, on March 1, 2017, the New York Department of Financial Service, which supervises banks, insurance companies and other financial service entities, issued a new set of regulations (23 NYCRR 500 *et seq.*), imposing new information safeguard requirements. *See* Kenneth Rashbaum, *Cybersecurity for Law Firms: Business Imperatives Update 2017*, New York Law Journal (March 6, 2017). The new regulatory requirements will apply to law firms as third party service providers, and will require firms to show that they have assessed their information safeguard protocols. The regulations also require that any agreements with law firms contain representations that the firm has cybersecurity policies and procedures regarding the encryption of nonpublic information in place. Law firms that represent financial services or health care clients will be most affected, but firms of all shapes and sizes would do well to familiarize themselves with these new regulatory requirements.

In addition to the imposition of civil and regulatory liability, a firm's reputation may suffer significant damage as a result of public, and potentially embarrassing, data breaches. Moreover, in light of the ethical guidance provided by the NYSBA and ABA ethics committees, attorneys could very well be the subject of disciplinary proceedings if they fail to adequately secure client data. While we are currently unaware of any disciplinary proceedings initiated in New York as a result of an attorneys being the subject of a cyberattack, such cases may arise as more and more data is stored online, and the number of cyberattacks increase. Attorneys would therefore be wise to familiarize themselves with the applicable ethical guidelines and be proactive with respect to securing their client's confidential information.

Sincerely,

The Forum by
Vincent J. Syracuse, Esq. (Syracuse@thsh.com)
Maryann C. Stallone, Esq. (Stallone@thsh.com)
Richard W. Trotter, Esq. (Trotter@thsh.com)
Carl. F. Regelmann, Esq. (Regelmann@thsh.com)
Tannenbaum Helpern Syracuse & Hirschtritt LLP

Continued on Page 60

Attorney Professionalism Forum
Continued from Page 56

QUESTION FOR THE NEXT ATTORNEY PROFESSIONALISM FORUM

I recently started a solo practice and my practice is growing slowly. A friend recently asked me to appear for him in court when his per diem attorney had a last minute emergency. I realized that while my practice is still growing, making occasional appearances as a per diem attorney might be a good way to bring in some additional fees. In hindsight, after making the appearance on behalf of my friend, I realized I never did a conflict check and didn't have a written arrangement as to my representation, and I am sure my friend's client didn't know who I was. Although I don't think anyone was concerned about this in the least, did I act improperly? I can't imagine attorneys that appear on a regular basis as per diem attorneys run conflict checks on a daily basis. But if I do this going forward, what rules do I need to consider when appearing as a per diem attorney. For example, do I need to have formal relationships with each of the attorneys or firms that I appear for? Are there certain types of cases I should reject if I am asked to appear? When I worked for my prior firm, I occasionally would show up for a conference expecting to resolve a discovery dispute only to discover that the opposing attorney sent a per diem attorney with no knowledge of the case or authority to act. It would drive me crazy. Am I exposing myself to professional liability even though I was just asked to show up for a routine conference? Any advice would be appreciated.

Yours truly,
Attorney Foraday

The Legal Writer
Continued from Page 59

Answers: Gender Neutrality

1. Use gender-neutral terms. Unless someone is really a sister or brother, replace "sister" or "brother" with "sibling." *Corrected version:* New Jersey is New York's sibling state.
2. This sentence isn't gender neutral. It uses the female pronoun. Making the noun plural is one way to make the sentence gender neutral. *Corrected version*: Judges can't be biased. They must be impartial. *Better version:* A judge can't be biased. A judge must be impartial.
3. This sentence isn't gender neutral. It uses a term reserved for a female. Eliminate "Madam." *Corrected version:* Justice Ruth Bader Ginsburg has been a United States Supreme Court Associate Justice since 1993.
4. This sentence isn't gender neutral. Eliminate the pronoun. *Corrected version:* Anyone comfortable speaking in public should be a litigator.
5. This sentence should substitute "man" for "person" or "human." *Corrected version:* Ben did what any person would have done: he told the truth.
6. The language in this sentence isn't parallel. *Corrected version:* The husband and wife robbed banks across the country.
7. Don't fix gender issues by internal disagreement. *Corrected version*: Good lawyers take their job seriously. *Or:* A good lawyer takes work seriously.
8. To use gender-neutral terms, avoid the suffix "-ess." Replace "waitress" with "waiter" or "server." *Corrected version:* The waiter (or server) was hesitant to testify.
9. Replace "con man" with "con artist" to make the sentence gender neutral. *Corrected version:* A convicted con artist will be arraigned tomorrow.
10. Use gender-neutral parallel language. *Corrected version:* "I now pronounce you husband and wife!" ■

Gerald Lebovits (GLebovits@aol.com), an acting Supreme Court justice in Manhattan, is an adjunct at Columbia, Fordham, and NYU law schools. He thanks judicial interns Alexandra Dardac (Fordham University) and Tamar Rosen (Benjamin N. Cardozo School of Law) for their research.

"I'm beginning to wonder if both you guys are lying."