



Pssst...Can Your Lawyer Keep a (Trade) Secret?

Insights

11.29.10

The American Bar Association's Commission on Ethics 20/20 (the "Commission") is examining whether technological advances are placing clients' confidential information at risk, and if so, what should be done about it. The Commission recently released an [Issues Paper](#) that identifies various risks presented by the increasing use of technology by the legal profession and solicits feedback on how to address these risks.

Once upon a time, this was a paper-based world. We took notes by hand, or typed letters on typewriters. But the world has changed, and it has changed dramatically. Data are increasingly generated, transmitted and retained in electronic form, and this has important implications for attorneys and clients involved in matters involving trade secrets and confidential information. When clients entrust their trade secrets and confidential information to their attorneys, they send it via e-mail or on a disc. What used to be maintained securely in a file cabinet under lock and key is now stored electronically either locally on devices such as servers, laptops, flashdrives or blackberries, and sometimes it is stored remotely on the internet via online storage vendors or internet email providers.

Remote storage of client data presents several concerns including unauthorized access to confidential client information by a vendor's employees or by hackers, a failure to adequately back up data, or insufficient data encryption. These risks are seemingly outside of a lawyer's control. In contrast, electronic storage of data on so-called "local" devices is subject to greater attorney control. For example, attorneys can utilize physical protections, passwords, and methods for deleting data remotely in the event that a device is stolen. Lawyers also can install appropriate safeguards against malware, and they can encrypt sensitive information.

Through its [Issues Paper](#), the Commission is reaching out to solicit input from the legal profession about the issues identified in the paper and to ask what obligations attorneys have to investigate and address these types of risks. Some attorneys, such as Larry Bodine at Apollo Business Development, are concerned because the Issues Paper on confidentiality risks was released concurrently with another paper addressing risks presented by lawyers' use of social media for marketing and advertising purposes. Bodine has criticized the Commission arguing that it is "quietly gathering support to choke off lawyer marketing" by having the Commission distribute its Issues Paper. According to Bodine, "We don't need more regulation, we need less." Bodine is concerned that "[n]ew ethics rules always start with little-known ABA committees that appear to be pursuing

input. What they are actually doing is collecting emails and letters in support of the Model Rules they want to promulgate.”

The Commission could not disagree more. In a recent [podcast](#) created by Commission Reporter Professor Andrew Perlman of Suffolk University Law School, Professor Perlman emphatically rejects the “belief that the papers were in some way designed to build support for new restrictions on lawyer advertising or were a first step to stifling lawyers’ use of social media as a form of marketing.” Noting that he was a primary drafter of the Issues Papers, Professor Perlman states that the Commission’s goal is merely to identify problems arising from the increasing use of technology by the legal profession and to seek “guidance as to possible solutions.” According to Perlman, the Commission promised to engage in significant outreach to the profession, and lawyers are encouraged to read the papers and send comments to the Commission. Instructions on how to submit comments are in the [Issues Papers](#) themselves.

Perlman adds that the papers do not contain any particular proposal at this time. There is no interest in keeping lawyers from using these types of technology. Rather, the Commission states that depending on the input received, its possible steps could range from drafting a white paper to provide lawyers with guidance to creating an online resource that periodically updates and describes existing practices and emerging standards. The Commission also acknowledges that it may propose amendments to the Model Rules of Professional Conduct.

Although the Issues Paper addresses items of obvious concern for practicing attorneys, it touches upon an issue that businesses should be asking themselves: Can your attorneys keep a secret? More importantly, can your attorneys keep a ‘trade secret’ secret?

Ensuring that your trade secrets are kept secret is not a new requirement. Forty-six states plus the District of Columbia have enacted a version of the [Uniform Trade Secrets Act](#), which provides that in order to be considered a trade secret, the owner of such information must make “efforts that are reasonable under the circumstances to maintain its secrecy.” While this legal rule is not new, perhaps its application in this context is novel. After all, clients rightly assume that lawyers will take steps to protect their confidences. As the Commission and this blog have recognized, the body of law concerning data privacy is rapidly growing. For example, [Massachusetts](#) recently adopted regulations establishing minimum standards for the protection of consumer data.

In short, businesses need to think about the many ways their confidential information is at risk. Internal controls on use and dissemination of confidential information may not be entirely sufficient. Businesses need to recognize that risks sometimes involve the handling of their data by third parties specifically entrusted for that purpose. Go ahead and ask your lawyer, can you keep a (trade) secret?

Michael R. Greco is a partner in the Employee Defection & Trade Secrets Practice Group at Fisher Phillips. To receive notice of future blog posts either [follow Michael R. Greco on Twitter](#) or subscribe to this blog's RSS feed.

Related People



Michael R. Greco
Regional Managing Partner
303.218.3655
[Email](#)