UT LAW CLE | THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

2018 Stanley M. Johanson Estate Planning Workshop

November 16, 2018
Austin, Texas

OF MICE AND METADATA– Ethics, Client Confidentiality, and the Duty of Competence in the Digital Age

Bernard E. ("Barney") Jones

Author Contact Information:
Bernard E. ("Barney") Jones
Attorney at Law
3555 Timmons Ln, Ste. 1020
Houston, Texas 77027

bjpub@bejlaw.com

713 621 3330

Table of Contents

Of Mice and Metadata–
Ethics, Client Confidentiality, and the Duty of Competence in the Digital Age

Bernard E. ("Barney") Jones

I.
INTRODUCTION; SCOPE OF PRESENTATION

This paper is a focused study of the electronic communication of confidential client information, including privileged information (collectively, "CCI"). Specifically, it concentrates on two recent ethics opinions, one ABA opinion and one Texas opinion, and the intersection of ethics and technology that they address. It begins with an analysis of the ethics opinions. It follows with a discussion of the technology of electronic communications and recommended "best practices" for protecting CCI contained in digital communications.

II.
THE RULES

A. ABA Formal Opinion 477R

Issued May 11, 2017 (revised May 22, 2017) by the ABA Commission on Ethics and Professional Responsibility (the "ABA Ethics Commission"), ABA Formal Opinion 477R ("ABA Op. 477R") concludes as follows:

> A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct *where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access*. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

(ABA Op. 477R, part V, p. 11, emphasis added). The opinion is well written and, in my view, required reading for all attorneys and paralegals. The opinion's actual conclusions – the rules it says we should follow – are not particularly striking. The foundations of the opinion are provocative.

1. IT'S OK TO COMMUNICATE CCI VIA THE INTERNET IF YOU'RE REASONABLY CAREFUL

Cooked down to its fundamental conclusion ABA Op. 477R simply says: "Be reasonable." It happens to say so in the context of electronic communication of CCI but it makes it clear that the conceptual conclusions it reaches are no different than those applicable to regular mail, telephone conversations and all other forms of communication involving CCI. And, as is the case with all rules based on a reasonableness standard, the opinion is light on specifics and safe harbors and can leave the reader feeling ill at ease, compelled yet again to follow a rule that is official and important yet rarely objective.

I am, however, unable to fault the opinion for its almost complete subjectivity because I agree with the authors' [implicit] view that, when dealing with the internet and computer technology, most black and white objective rules would likely be obsolete almost as soon as written.

a. Electronic Communication of CCI is OK

However self-evident it may be, the opinion's threshold conclusion is too important not to mention: *Lawyers are authorized to use the Internet and other electronic means for communicating with and about their clients*: Thus, it is OK to email, to text, to use online file sharing – that is, it *can* be.

b. "Reasonable Efforts" to Protect CCI Are Always Required

"The Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates . . .." (ABA Op. 477R, part I, p. 2) Thus, the lawyer's duty of confidentiality regarding electronic communications is the same as that regarding non-electronic communications: In all communications by any means the lawyer must always take "reasonable efforts to prevent inadvertent or unauthorized access." Owing to the inherent differences between various forms of communication, the particular efforts to prevent inadvertent disclosure of, e.g., regular mail and email, are, of course, completely different. But both are judged by the same standard of reasonableness.

c. Generally, "Reasonable Efforts" to Protect CCI Are All That's Required

Observing that the internet is rife with "nefarious actors" (*Id.*), the opinion recognizes what I consider to be a fundamental truth, that the question is not "if" but "when" hacking and data loss will occur. It follows that no lawyer (nor any other person) can fairly be held accountable as a guarantor of confidentiality, and the opinion makes this point clear. (*See also* Texas Professional Ethics Committee Opinion 648, April 2015, "the risk an unauthorized person will gain access to confidential information is inherent in the delivery of *any* written communication including delivery by the U.S. Postal Service, a private mail service, a courier, or facsimile", emphasis added)

The opinion notes that Model Rule 1.6(a) requires that "[a] lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise; and that Model Rule 1.6(c) requires that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." (MODEL RULES OF PROF'L CONDUCT R. 1.6(a), (c) (2016)). Then the opinion expressly states:

> The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

(ABA Op. 477R, part III, p. 4, quoting from MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2016))

d. What Constitutes "Reasonable Efforts" Depends on the Circumstances

The duty of care being a reasonableness standard, not an objective rule, the opinion expressly refuses to provide a "hard and fast rule" for what constitutes reasonable efforts. Instead, adopting language from the ABA Cybersecurity Handbook, the opinion concludes as follows:

> [The reasonable efforts standard] rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.

(ABA Op. 477R, part III, p. 4, quoting from JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 7 (2013), at 48-49)

e. "Reasonable Efforts" Means "Extraordinary Efforts" in Certain Cases

From the literal wording of the opinion's summary (quoted above) one might infer that it proscribes two rules for the protection of CCI: (1) Reasonable efforts are required in ordinary situations but (2) "special security precautions" are required in extraordinary situations. From the entirety of the opinion it seems clear that the authors' embrace a single "reasonable efforts" rule under which nominal efforts are sometimes reasonable and, other times, the only reasonable course is to employ extreme efforts.

Thus, it seems to me obvious that if special security precautions are "required by an agreement with the client or by law" or "the nature of the information requires a higher degree of security", it would be patently *unreasonable* to employ only nominal precautions.

f. Factors Relevant to the Reasonable Efforts Determination

The opinion provides the following nonexclusive list of factors to guide lawyers in making a "reasonable efforts" determination (ABA Op. 477R, part III, p. 4, again quoting from MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2016)):

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

The first two factors impose the duty: The existence of information that is sensitive and at risk of being disclosed gives rise to a duty to take efforts to prevent its disclosure.

The remaining three factors temper the duty. They supply the provisos, the exceptions that soften what would otherwise be an almost absolute duty. They confirm that only *reasonable* efforts are required. Efforts that could virtually guaranty protection from disclosure but that would be excessively expensive,

Title search: Of Mice and Metadata: Ethics, Client Confidentiality, and the Duty of Competence in the Digital Age

First appeared as part of the conference materials for the
2018 Stanley M. Johanson Estate Planning Workshop session
"Of Mice and Metadata: Ethics, Client Confidentiality, and the Duty of Competence in the Digital Age"