IOWA ETHICS OPINION

January 28, 2015

A LAWYER SENDING OR RECEIVING SUBSTANTIVE COMMUNICATIONS WITH A CLIENT VIA E-MAIL OR OTHER ELECTRONIC MEANS ORDINARILY MUST WARN THE CLIENT ABOUT THE RISK OF INTERCEPTION INCLUDING THE USE OF A COMPUTER OR OTHER DEVICE, OR E-MAIL ACCOUNT, TO WHICH A THIRD PARTY MAY GAIN ACCESS.

NICK CRITELLI, Chair
Iowa State Bar Association
Ethics and Practice Guidelines Committee[1]

IOWA ETHICS OP. 15-01

Preface

Eighteen years have passed since the Committee last addressed the use of e-mail communication by lawyers. With passing time, electronic communication has become ubiquitous in all sectors of modern society. With advancement in technology electronic communication has expanded to include modes of transmission, like texting, and other forms of instantaneous messaging that that were beyond comprehension then as future modes will be eighteen years hence. The time has come to revisit our prior opinions and provide guidance for the present and foreseeable future.

Introduction

In 1996 the Committee determined that electronic communication was an acceptable form of attorney-client communication provided that it met certain security standards. Iowa Ethics Op. 96-01 provided that:

> III. Pure inter-exchange of information or legal communication with clients is an exception to Division I of this opinion, but with sensitive material to be transmitted on E-mail counsel must have written acknowledgment by client of the risk of violation of DR 4- 101 which acknowledgment includes consent for

[1] Nick Critelli, Chair, David Phipps, Maureen Heffernan, J.C. Salvo, Matthew Hartman McKinney, David Beckman, Sam Langholz, Stan Thompson, Andrew Heiting-Doane, Paula L. Roby, Andrew C. Abbott, Art Cady, Sara Laughlin; ex officio: Joe Feller, President, ISBA, Dwight Dinkla, Ex. Dir. ISBA. The Iowa State Bar Association Committee on Ethics and Practice Guidelines was established in response to an April 21, 2005 Resolution by the Iowa Supreme Court. Its opinions are advisory only.

communication thereof on the Internet or non-secure Intranet or other forms of proprietary networks, or it must be encrypted or protected by password/firewall or other generally accepted equivalent security system.

A year later that requirement was modified by Iowa Ethics Op. 97-1 by eliminating the phrase "or it must be encrypted or protected by password/firewall or other generally accepted equivalent security system." The rule, as it stands, is that before using electronic communication a lawyer must obtain a written acknowledgement by the client of the risks inherent in Internet communication and an agreement or consent to its use.

Present Iowa Position

Reading the two rules in tandem reveals that the 1996 opinion required written acknowledgement and consent OR encryption or password protection whereas the 1997 opinion eliminated the safe harbor provision of encryption or password protection and relied solely on acknowledgement and consent.

In 2011 this Committee addressed a similar situation in "Software as a Service – Cloud Computing" in Iowa Ethics Op. 11-01. We adopted a due diligence approach to the use of technology, such as storing confidential client matters on computer servers maintained off site by third parties. We based our opinion on Comment [17] to Iowa R. Prof'l. C. 32: 1.6:

> [17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

We adopted a:

> " ....reasonable and flexible approach to guide a lawyer's use of ever-changing technology. It recognizes that the degree of protection to be afforded client information varies with the client, matter and information involved. But it places

> on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly."

ABA Position

On August 4, 2011 the ABA issued ABA Formal Opinion 11-459 defining a lawyer's duty in sending or receiving substantive communications with a client via e-mail or other electronic means. Because electronic communication has become ubiquitous, clients are often not sensitive to security concerning attorney-client communication. Frequently, they will communicate using employer furnished, multi-user or public computers without thought about security of the communication.

ABA Formal Op. 11-459 opined:

> Given these risks, a lawyer should ordinarily advise the employee-client about the importance of communicating with the lawyer in a manner that protects the confidentiality of e-mail communications, just as a lawyer should avoid speaking face-to-face with a client about sensitive matters if the conversation might be overheard and should warn the client against discussing their communications with others. In particular, as soon as practical after a client-lawyer relationship is established, a lawyer typically should instruct the employee-client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney-client communications, because even seemingly ministerial communications involving matters such as scheduling can have substantive ramifications.

The ABA opinion concluded by requiring a lawyer to warn of the risks interception inherent in electronic communication:

> A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, to which a third party may gain access. The risk may vary. Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client.

Conclusion

ABA Formal Opinion 11-459 requires a lawyer to " warn the client about the risk of sending or receiving electronic communications using a computer" but stops short of requiring a written acknowledgement and consent as required by Iowa Ethics Ops. 96-

01 (written acknowledgement and consent OR encryption) and 97-01 (written acknowledgement and consent). By requiring written client acknowledgement and consent the lawyer is provided with much safety if inadvertent or intentional disclosure occurs by hackers. We recognize that most lawyers embody the written acknowledgment and consent in their engagement agreements. Likewise we recognize that Iowa Ethics Op. 11-01 places a duty of due diligence on the lawyer regarding encryption for sensitive information. See also Iowa Ethics Op. 14-01 concerning computer security. These are all best practices and a lawyer would be wise to adopt them as a matter of practice. However the ABA position is more attuned to the present reality of practice. Consequently Iowa Ethics Ops. 96-01 and 97-01 are withdrawn and instead we adopt ABA Formal Opinion 11-495. However in doing so we warn that lawyers should constantly be mindful of the inherent risks involved with any type of communication, be it digital or analogue or even oral. The lawyer must engage in an analysis involving time, place and manner. To borrow a slogan from WWII, "loose lips sinks ships."

OPINION

A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, to which a third party may gain access. The risk may vary. Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client.