Global Information Assurance Certification Paper

Making a Case for E-mail Encryption in Legal Settings
Thomas S. Martin
November 19, 2000

> "Of course, most lawyers claim that encryption is too hard to use. These are the same people who would spend days learning how to program the presets in their BMW."
>
> "The law and the legal profession, perhaps more than any other institutions, resist change."

The purpose of this paper is to enable an IT or security professional to present a reasonable argument in favor of e-mail encryption to attorneys or law firm principals. Recent developments, in particular an influential committee opinion concerning attorney-client privilege, have most U.S. attorneys convinced that e-mail encryption is unnecessary; possibly a useful tool but not something to require under a policy controlling internal and external communications. A security professional attempting to "sell" encryption as part of a proposed policy (and encryption should only be considered as part of a larger, defense-in-depth approach to information security) should be aware of the issues that the lawyers may raise in opposition.

I. Client Confidentiality and the Attorney-Client Privilege

After a slow start, the legal profession has adopted electronic mail (e-mail) with a passion: ease of use and rapid ubiquity have made it an indispensable tool for communication with clients. The profession has now come up against the same question that presented itself with the wide scale adoption of the telephone: is the medium secure enough for confidential communications between attorney and client? Can my client assert the attorney-client privilege in an e-mail?

Attorney-client privilege is a subset of the larger requirement for confidentiality.

It is also the oldest established rule protecting confidentiality. The privilege essentially protects certain communications between a lawyer and client from being disclosed or introduced as evidence in a legal proceeding. The modern purpose of the privilege is to promote free and open communication between the attorney and the client.

Rules of Professional Conduct exist in every jurisdiction, usually administered by the state Bar Association as well as by statute, and in the U.S. are based on Model Rules arrived at by a committee of the American Bar Association (ABA). The ABA Model Rules of Professional Conduct, last amended in 1998, form the basis for most statutory professional conduct rules for lawyers.

Model Rule 1.6(a) defines "confidential client information" as "information relating to the representation of a client" under which:

> "(a) a lawyer shall not reveal information relating to representation of a client unless a client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation."

To add difficulty to the confidentiality issue, it is still considered a complex concept and not fully understood. An important element of the confidentiality equation is that not every communication is equal. The attorney-client privilege and the larger confidentiality requirement both assume that some communications are normal to the course of business, for example, and don't require security precautions. The "reasonableness" standard is applied to any analysis. A lawyer might actually harm his client's ability to assert the attorney-client privilege by labeling every communication privileged.

II. Formal Opinion 99-413

In 1999, the American Bar Association's Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 99-413, in which they presented an analysis of the various kinds of electronic communications in the light of the attorney-client privilege and confidentiality and concluded:

> "The Committee believes that e-mail communications, including those sent unencrypted over the Internet, pose no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy."

On its face, the opinion reads as a straightforward statement that encryption is unnecessary to preserve the attorney-client privilege, because "there is a reasonable expectation of privacy in (e-mail's) use." This is how most attorneys have chosen to regard the opinion, which has been widely publicized. The Formal Opinion also reflects the findings of a number of local bar associations' ethics opinions, mostly issued in the 1997-1998 time frame.

There are several serious problems with the analysis within ABA 99-413. The first is a loophole built into its wording. At its conclusion, the opinion states that unencrypted e-mail may be too insecure for information that is "highly sensitive." This exception could 'swallow the rule;' every client will probably assert that his information was highly sensitive in the event of a malpractice lawsuit.

ABA 99-413 seriously underestimates current threats to e-mail. It states:

> "(P)ractical constraints on the ability of third parties and ISPs to capture and read Internet e-mail lead to the conclusion that the user of Internet e-mail has a reasonable expectation of privacy." (A brief discussion of packets and fragmentation follows.)

No mention is made of such technology as the FBI's Carnivore program, in existence at the time of drafting, which monitors large volumes of e-mail traffic (with the stated objective of filtering out only the messages that the FBI has some legal justification for monitoring.) Carnivore uses technology that is fairly unsophisticated by today's standards. Furthermore, commercial vendors of snooping software abound, e.g. SRA International's Assentor©, designed for the financial services industry, which performs natural language filtering of e-mail.

A last, rather curious part of the ABA's analysis in 99-413 is the statement that intercepting an e-mail transmission would be considered wiretapping under the Electronic Communications Privacy Act (ECPA) and therefore a crime, and would thus act as a deterrent to the interception of e-mail. The flaws in this reasoning seem fairly evident: criminals are unlikely, by definition, to be deterred by the prospect of breaking the law. The hacking community flourishes worldwide despite the existence of such laws as the ECPA.

ABA 99-413 found that transmission of unencrypted e-mail after consultation with the client, advising the client of the risks involved, was a reasonable way to exchange client information. In this author's opinion, the current threats to e-mail security, including the commercial availability of interception software, detract from the reasonableness of the expectation of privacy, and make encryption itself a reasonable solution for protecting certain confidential e-mail transmissions.

In the context of a security policy, the key to making sense of this complex situation seems to be (a) to establish guidelines for what is considered confidential, and (b) to require encryption for e-mail communications that fall within those guidelines.

III. Other Considerations: Best Practices and Marketing

The main objection of a typical lawyer to encryption would probably be based upon a cursory or incomplete understanding of ABA 99-413, which has received wide publicity. A more compelling argument for the inclusion of e-mail encryption into standard security procedures would be hard to prove to a lawyer, but is nonetheless valid: the inclusion of encryption into a firm's practices and policies is a good marketing tool. It would send a statement to clients that the firm or lawyer was technologically current and considered their clients' security important.

Conclusion

Historically, the American legal community has been slow to adopt advances in information technology. It is axiomatic to IT professionals (the author included) with law firms as their employers or clients, that getting their lawyers to agree to an upgrade or new purchase is fraught with danger and woe. The reasons behind this are often baffling, since American lawyers and their counterparts around the world have benefited as much from the changes in office automation over the last 20 years as any businesses in any industry.

When lawyers do adopt, they tend to be enthusiasts, with exaggerated faith in new gadgets. Encryption software has had security vulnerabilities and will probably continue to do so, and it, like any other technology, is as strong as its weakest link, the end-user. Training, maintenance and upgrading, and clear guidelines for use should be an inseparable part of any implementation of encryption software. And finally, any encryption solution should be implemented only as part of an overall defense-in-depth strategy.

References

i. Heels and Klau, Law Law Law on the Internet: The Best Legal Websites and More (American Bar Association

Press, 1998)

ii. Matthews, "Encoded Confidences: Electronic Mail, the Internet, and the Attorney-Client Privilege" 45 Kan. Law Rev. 273, 281

iii. Legal settings differ in many respects. Corporate legal departments often are covered by company-wide policy that dictates use of security measures. However, corporate departments often function as a small (or large) law firm within the greater setting, especially when it comes to matters unique to their practice of law. Therefore, some or all the following also applies to legal departments within companies.

iv. The modern consensus is that telephones are sufficiently secure. ABA Formal Opinion 99-413, discussed infra, notes that it is "undisputed that a lawyer has a reasonable expectation of privacy in the use of a telephone" and that "the attorney-client privilege applies to conversations over the telephone as long as the other elements of the privilege are present." Also see Peter R. Jarvis & Bradley F. Tellam, High-Tech Ethics and Malpractice Issues 7 (1996)

v. see Matthews, supra at 280

vi. id. At 282

vii. See e.g. State Bar of California Rules of Professional Conduct (http://www.calbar.org/pub250/1995rpc.htm) last updated 1/1/00

viii. ABA, Annotated Model Rules of Professional Conduct (1999, American Bar Association)

ix. CA Bus. & Prof. Code 6068(e) states that it is every attorney's duty "to maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client."

x. In California, the issues around confidentiality have been extensively debated. In 1996, a State Bar committee was formed to review Bus. & Prof. Code 6068(e) and participants noted, among other things, that California has no rule which defines "confidentiality" for the purposes of instructing the lawyer and law office staff what information must be kept confidential, or what must not be told to anyone not involved the representation of the client. (http://www.calbar.org/2ent/3con/4con1/08-01.htm)

xi. See Rice, Attorney-Client Privilege in the United States 2d (2000, West Publishing Group)

xii. ABA STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY Formal Opinion No. 99-413 (March 10, 1999) (http://www.abanet.org/cpr/fo99-413.html)

xiii. See, e.g., Alaska Bar Ass'n Op. 98-2 (1998) (lawyers may communicate with clients via unencrypted e-mail; client consent is unnecessary because the expectation of privacy in e-mail is no less reasonable than that in the telephone or fax); D.C. Bar Op. 281 (1998) (lawyers' use of unencrypted e-mail is not a violation of duty to protect client confidences under District of Columbia Rule of Professional Conduct 1.6); Ky. Bar Ass'n Ethics Comm. Advisory Op. E-403 (1998) (absent "unusual circumstances" lawyers may use e-mail, including unencrypted Internet e-mail, to communicate with clients)

xiv. "Hackers who gain "root" over a system through which your e-mail passes (not that hard to do in many cases) can do exactly the same thing that the FBI is doing--and their intentions may be much less benign than those of the FBI." Lawson, "E-Mail Security: A Reality Check" Sept. 2000 (http://www.llrx.com)

xv. http://www.sra.com/commercial/fs_assentor.html

xvi. The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), amended the Federal Wiretap Statute of 1968 by extending its scope to include "electronic communications." 18 U.S.C.A. (2510, et seq.) (1998) The ECPA now commonly refers to the amended statute in its entirety. The ECPA provides criminal and civil penalties for the unauthorized interception or disclosure of any wire, oral, or electronic communication. 18 U.S.C.A.

xvii. Some law firms are already incorporating at least the option to encrypt into their communications with clients and potential clients. The e-mail software at the firm of Seltzer Caplan Wilkins & McMahon automatically inserts the following footer on all outgoing e-mail messages:

"SCWM Information Services <scwm.com>" made the following annotations on 10/12/99 11:57:27

This message was sent unencrypted. This firm has the ability to exchange encrypted email at no cost to our clients. If you are interested in obtaining this service please send email to scwm.com"

xviii. See Peter Krakaur's article "People, Not Products, Protect Client Confidences; Why You Should Not Rely on Encryption to Fulfill Your Ethical Obligations," written for the LLRX.com Symposium on E-Mail Security (http://www.llrx.com/email/) In it, he notes several instances of security vulnerabilities in encryption products, including PGP. Krakaur generally supports the reasoning behind ABA 99-413, although he supports the use of encryption software in some circumstances.

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS