

## World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

### Security & Surveillance

#### What Legal Standards Apply to the Securing of Lawyer-Client Digital Communication?

**Mark Starcher**  
Scanmark Ltd.  
McLean, VA.

Reprinted from the October 2005 issue of BNA International's  
*World Data Protection Report*



[www.bnai.com](http://www.bnai.com)

# What Legal Standards Apply to the Securing of Lawyer-Client Digital Communication?

*By Mark Starcher, President, Scanmark Ltd., McLean, VA. The author is a member of several state bars in the United States. Scanmark Ltd. provides security technology services to private and governmental entities in the United States (www.scanmark.com).*

Use of digital communication services<sup>1</sup> has dramatically altered the means by which lawyers and clients communicate. Electronic mail (“e-mail”) particularly, given its long-standing use (in “Internet time”<sup>2</sup>) and acceptance, is commonplace in lawyer-client communications. Other digital communication services such as instant messaging (IM), IP telephony (VOIP), and video conferencing are rapidly gaining acceptance as telecommunication services and applications mature. And use is not restricted to the law office – wireless digital devices such as cell phones, personal digital assistants (PDAs), and WiFi (Wireless Internet Access) allow the business of law to be conducted anywhere at any time. Lawyers’ use of digital communication services over the next few years will increase because of the concomitant cost savings from reduced travel, communication and delivery costs.

The profession’s adoption of these communication services comes at a time when digital security is making front-page news. Identity theft, spoofing, spamming and Internet scams have become commonplace. Information security, once considered a discipline reserved for techies, has now become a necessary business process that requires the involvement of anyone using digital services.

The technical standards to which the profession is being held today are, at best, inconsistent. Use of digital communications by lawyers might be perceived as “ethical” but could be violating other legal and regulatory constraints regarding the security of information.

This scenario is understandable given the “culture clash” between the legal profession and the Internet generation. “Legal guidance” on ephemeral information technology concepts (that typically have a useful life measured in months) does not exist or is valid only in a historical context. Lawyers are always in catch-up mode when addressing technology. Thus, it comes as no surprise that there exists a hodgepodge of dated legal, regulatory and ethical precedents that leave an unclear picture regarding lawyers’ responsibilities in securing digital communications. Recent legislative action in the United States has further muddled the picture by mandating security practices for certain types of digital information.

This article reviews the current patchwork guidance surrounding the security of lawyer-client digital communication in the context of e-mail and document attachments.

## E-Mail and Attachments (A Technology Overview)

An estimated 93 percent of U.S. lawyers surveyed have access to electronic mail to some degree, with more than 80 percent using e-mail services to communicate work product with clients.<sup>3</sup>

Use of Internet-based e-mail services requires that messages travel over a public network using a data transmission protocol called Internet Protocol (IP).<sup>4</sup> The most widely used mail application is the Simple Mail Transport Protocol (SMTP).<sup>5</sup> This protocol uses a “store and forward” method to deliver messages to a recipient asynchronously. The protocol uses routing information to break up a message into a number of packets and delivers those packets to a recipient in the most efficient manner given current traffic patterns on the public network. In some instances, parts of the same message will use different routes to reach the recipient after which the message is reconstructed and displayed on the recipient’s computer.

The SMTP application breaks up a message and sends the message packets across the public network in “clear text”, *i.e.*, the message packets can be read by anyone with access to the message stream. Access to the message stream can be initiated using commercially available software devices called “sniffers” at any point during message transmission when a packet passes through a routing device. These software programs allow a person to reconstruct and read typical e-mail traffic. A message packet may travel through multiple routing points before delivery to the recipient. These same e-mail messages can be accessed at the recipient’s or sender’s computer through a variety of hacking tools including Internet worms, viruses, and Trojan horses which are designed to compromise and obtain access to any information residing on a “hacked” computer.<sup>6</sup>

The analogy typically drawn with the use of SMTP e-mail is sending a postcard through the mail. Anyone who happens to see the postcard can read the contents of the card. This presents a problem for privileged communication between client and lawyer.

E-mail attachments are equally important in client communication. The textual document or spreadsheet forwarded to the client typically contains the bulk of the message, whether it be a draft complaint, deposition, or suggested contractual language. The attachments are typically transported using Multipurpose Internet Mail Extensions (MIME).<sup>7</sup> This collection of protocols identifies the underlying application and allows the file to be delivered to the recipient in binary form (*i.e.*, the content is encoded in the particular application’s format). Anyone that intercepts the message and attachment can read the binary attachment if they have the associated application.

The questions facing the legal profession are what standards should be applied to securing digital communication. Should e-mail be routinely encrypted, should e-mail servers, office networks and lawyer computers be secured? If so, what standard(s) of reasonable care should be applied? Broadly speaking, there are three competing standards which address the attempts to enforce digital security:

- ethical guidelines;
- the lawyer-client privilege; and
- statutory and regulatory proscriptions.

## Legal Ethics and Unsecured E-Mail

Is it “ethical” for a lawyer to communicate with clients via an unsecured e-mail protocol?<sup>8</sup> Early guidance in the United States concluded that the SMTP protocol was inherently insecure and lawyers should consider the use an encryption device to secure the communication channel or obtain advance consent from the client to use an unsecured communication device.<sup>9</sup>

These early opinions were subsequently reviewed and revised based on a perception that the use of Internet e-mail created a reasonable expectation of privacy on the part of the lawyer and the client and any interception of the e-mails was in violation of Federal law.<sup>10</sup>

In 1999, the American Bar Association issued Formal Opinion 1999-413, concluding that unencrypted e-mail could be forwarded to clients, noting that the privacy rights accorded to commercial mail, landline telephonic transmission and facsimiles were also applicable to Internet e-mail.<sup>11</sup>

A recent Arizona State Bar Opinion appears to come full circle in the rationale regarding digital communication, concluding that a lawyer must take “competent and reasonable” steps to assure that a client’s confidences are not disclosed to third parties.<sup>12</sup> Notably, the opinion discusses how the practice of law has changed since 1997 – the date of an ethics opinion allowing the use of unencrypted e-mail was issued in Arizona:

“However, it is also important to note that both the law and the practice have changed markedly since 1997. Obviously, the use of e-mail and cellular telephones has significantly expanded since 1997. Moreover, the use of the Internet in businesses of all kinds – including the practice of law – has exploded”.

Although the opinion is directed towards the safeguarding of client information stored at the lawyer’s offices, its tone is clear – lawyers are under an ethical duty to take “reasonable precautions” and “act competently” to protect client confidences.

### A Different Standard for Security under the Lawyer-Client Privilege

A separate legal standard exists for the evidentiary question of whether a client has waived the lawyer-client privilege with respect to work product and communications. This is distinct from the ethical confidence question, and involves a different analysis (e.g., “is there a reasonable expectation of privacy?”).<sup>13</sup>

In the case of e-mail or electronic communications, courts look to several types of disclosure to gauge whether there is a reasonable expectation of privacy. In the case of stolen information, courts have recently modified a long-standing evidentiary rule and allowed the lawyer-client privilege to maintain even where information has been stolen.

Nonetheless, the privilege, as described under Proposed Rule 503 of the Federal Rules of Evidence goes on to note:

“. . . Unless intent to disclose [an otherwise privileged communication] is apparent, the lawyer-client communication is confidential. *Taking or failing to take precautions may be considered as bearing on intent. . . .*” (Emphasis added).

This approach has been adopted by at least one U.S. Court<sup>14</sup> under which the general rule does not absolve the client and lawyer from taking precautions to protect communication.

However, this “modern rule” does not wholly relieve the lawyer or his client from taking precautions against theft and disclosure. The court held that preservation of the privilege does not “in any way reduce the client’s need to *take all possible precautions to insure confidentiality*”. [91 F.R.D. at 260 (quoting *2 Weinstein’s Evidence*, 503(b)(2)) (Emphasis added).]

The modern rule is clear that precautions must be taken by both lawyer and client to prevent the theft of confidential communications and preserve the privilege.<sup>15</sup>

### Statutory Provisions Impose Additional Standards of Care

To further complicate the security issues, recent legislative action in the United States has created further requirements with respect to certain types of information that may impose additional duties on lawyer-client communications.

### HIPAA E-Mail Security

The enactment of the Health Insurance Portability and Accountability Act (HIPAA) mandates that anyone dealing with health care related information must provide evidence of technical security services to guard data integrity and technical security mechanisms that prevent unauthorised access to information that is transmitted across an internal network or across the Internet.<sup>16</sup>

This regulation is applicable to lawyers and clients that pass medical-related information. These regulations provide that network controls such as firewalls, intrusion detection systems and other network devices must be installed to secure information stored at the lawyer’s offices. Moreover, these regulations provide that information must be protected whenever patient-identifiable information is sent via e-mail –whether it’s a message being sent between a doctor and patient, or between a lawyer and his client with medical issues.<sup>17</sup>

### Sarbanes-Oxley Act: Section 404

Section 404 of the Sarbanes-Oxley Act 2002 (SOX) provides that publicly-traded companies must show that they have established effective “internal control” structures for accurate and complete financial reporting. In addition, the company must provide evidence of an annual assessment of the internal controls, validated by a public accounting firm. Part of the assessment includes management review and appreciation of information technology security policies.

Although regulatory guidance on section 404 is scant, lawyers dealing with those firms subject to SOX (typically publicly-traded companies) will likely be subjected to internal control security reviews regarding the confidentiality of client information under the lawyer’s custody. This will include a review of in-house security measures as well as the means by which information is passed between client and lawyer.<sup>18</sup>

## Conclusions: Lawyer-Client Digital Communication

The uncertainty surrounding the security standards for lawyer-client digital communications is tied to the rapid technological change experienced by the legal profession over the past 10 years. There seems little doubt that future lawyer-client collaboration will be electronic in nature and will be conducted over increasingly hostile public communications networks.

Although “head in the sand” legal professionals will argue for the retention of existing security measures for digital communications, forward-looking firms will realise that building a security framework that protects client information (both in transit and locally) will provide long-term insurance against costs associated with legislative and regulatory changes regarding data integrity. Moreover, investing in a digital security framework today may allow firms to gain a competitive advantage over those legal professionals that are slow to embrace digital security technology.

- 1 Digital communication services are defined for purpose of this article to include electronic mail (e-mail) services using the Internet Simple Mail Transport Protocol (SMTP), instant messaging services provided by a variety of commercial enterprises, Short Message Services (SMS), Internet Protocol (IP) telephony (VOIP), and IP video services.
- 2 For a definition of this term, see [http://en.wikipedia.org/wiki/Internet\\_time](http://en.wikipedia.org/wiki/Internet_time). The meaning is similar to that of a “New York minute”.
- 3 See [www.abanet.org/tech/ltrc/publications/lomar\\_whatshotnot2004.html](http://www.abanet.org/tech/ltrc/publications/lomar_whatshotnot2004.html) for technology use figures for the years 2003-04.
- 4 Private e-mail networks that use proprietary standards or point-to-point telecommunication resources are not reviewed in this article.
- 5 For further information on the SMTP protocol, see <http://en.wikipedia.org/wiki/SMTP>. For guidance on setting up and running an SMTP service, see *Special Publication 800-45*, National Institute of Standards and Technology (NIST), September 2002, available at <http://csrc.nist.gov/publications/nistpubs/800-45/sp800-45.pdf>.
- 6 *A.C.L.U. v. Reno*, 929 F. Supp. 824, 834 (E.D. Pa. 1996), *aff'd* 521 U.S. 844 (1997) (“Unlike postal mail, simple e-mail is not ‘sealed’ or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted).”)
- 7 See <http://www.webopedia.com/TERM/M/MIME.html> for further information on the MIME protocols.
- 8 “A lawyer shall exercise *reasonable care* to prevent his employees, associates, and others whose services are utilized by him from disclosing or using confidences or secrets of a client...” (Emphasis added). American Bar Association Model Rules of Professional Conduct (1998), Model Rule 1.6.
- 9 See *Lawyers On Line: Ethical Prospectus in the Use Of Telecomputer Communications*, ABA Standing Committee on Lawyers’ Responsibility For Client Protection (1986). State Bar Opinions echoed the concerns regarding the security of e-mail transmissions. See, e.g., Tennessee Board of Professional Responsibility Opinion 98-A-650, available at [www.tba.org/news/encrypt.html](http://www.tba.org/news/encrypt.html), Iowa Ethics Opinion 96-1 1996, South Carolina Ethics Opinion 94-27 (1995), and North Carolina Ethics Opinion 215 (1995).
- 10 See, e.g., State Bar Ass’n of North Dakota Ethics Comm. Op. No. 97-09 (9/4/97); Illinois State Bar Ass’n Advisory Op. on Professional Conduct No. 96-10 (5/16/97); Arizona State Bar Ass’n Formal Op. No. 97-04 (4/4/97); South Carolina Bar Ethics Advisory Comm. Op. No. 97-08 (6/97) (overruling South Carolina Bar Ethics Advisory Comm. Op. 94-27, *supra*); and Vermont Advisory Ethics Op. No. 97-5.
- 11 American Bar Association Standing Committee on Ethics and Professional Responsibility, Formal Opinion No. 99-413 (March 10, 1999), available at [www.abanet.org/cpr/fo99-413.html](http://www.abanet.org/cpr/fo99-413.html). The opinion noted that under the Electronic Communications Privacy Act of 1996 (ECPA), 18 U.S.C. §2510, *et seq* interception of an electronic communication as defined in the act subjects the interceptor to the act’s penalties.
- 12 See State Bar of Arizona Ethics Opinion No. 05-04, July 2005, available at [www.myazbar.org/Ethics/pdf/05-04.pdf](http://www.myazbar.org/Ethics/pdf/05-04.pdf).
- 13 See Krakaur, *Treat E-mail Like Other Communications: An Argument Against Mandatory Encryption of Lawyer-Client Communications*. Available at [www.llrx.com/features/e-mail.htm](http://www.llrx.com/features/e-mail.htm). This article was written prior to the release of the ABA ethics opinion (as mentioned above).
- 14 *Suburban Sew ‘N Sweep, Inc. v. Swiss-Bernina, Inc.*, 91 F.R.D. 254 (N.D.Ill. 1981).
- 15 See Arizona Ethics Opinion, *supra*, note 12, at page 5.
- 16 These requirements are set forth in the following HIPAA regulations:
  - 45 CFR Part 142, § 142.308 (c). “Technical security services to guard data integrity, confidentiality and availability.” These are processes that protect information and control individual access to information.
  - 45 CFR Part 142, § 142.308 (d). “Technical security mechanisms.” These are controls that prevent unauthorised access to information that is transmitted across an internal network or across the public Internet.
- 17 See “HIPAA” Hiccups – Privacy Standards for U.S. Health Care Information Force Data Protection Enhancements, *World Data Protection Report* (August 2002).
- 18 The Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq* provides that certain regulated financial institutions and related entities must provide for the retention and safe storage of e-mail communications. This provision is not reviewed in this article.