

Security Interrupted:
A Simple Guide to Protecting Your Legal Correspondence

I. You've Already Taken the First Step.

You're here because you understand that security is important to your very busy practice or business. Thank you for taking to the time to review this short book, as together we demystify the topic of Internet security for the practice of law.

You may be thinking: "regular email is sufficient for my practice or my business's legal correspondence." The truth is, sometimes you're right. If you are sending a quick note about where to meet for lunch, or an invitation to the next firm event, you're entirely safe with email—no further thought required. However, the moment the conversation turns to substantive business or legal matters, you may need to rethink your position. This process requires a basic understanding of how email works, which we will cover here, and which you can explore in more detail at www.emailisdangerous.com.

*But wait, isn't all of this security talk over-stated? Sometimes, yes—and it is wise to be cautious when new technologies or solutions are proposed. But make no mistake, the underlying security issues are very real. For the attorney who accidentally emails private information to the national press,¹ the potential client who transmits sensitive contracts or personal information to counsel, or the lawyer who sends the subsequently-intercepted litigation strategy out for review, security *really* matters.*

II. The Dangers Are Real to Your Data and Their Trust.

Internet security breaches are well documented, and occur on a regular basis.² As customers and clients become more aware of the dangers presented to their data, they can be expected to become more selective about who they trust. With trust at the center of every attorney-client relationship, to be concerned about who trusts you is to be concerned about the viability of your practice or business.

¹ See, e.g., ABA Journal, "High-Profile Skadden Litigator Goofs, Sends Private E-mail to Reporters," *a v a i l a b l e* at http://www.abajournal.com/weekly/high_profile_skadden_litigator_goofs_sends_private_e_mail_to_reporters (Feb. 21, 2008).

² See Privacy Rights Clearinghouse, A Chronology of Data Breaches, at <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (updated Aug. 7, 2009) (listing numerous data breaches and stating that over 250,000,000 records containing sensitive personal information have been involved in security breaches in the United States since January 2005).

How can traditional email damage my client's trust? In two ways. First, there is a growing possibility that offering traditional email as the only means of online communication with you will deter progressive, Internet-savvy clients from sending business your way.³ Second (and more frightening) is the possibility that your client's or business's most sensitive information—social security numbers, bank routing numbers, marketing strategies, financial data (etc.)—could be compromised in an instant. If this happens as a result of online correspondence with you, everyone loses.⁴

Can email revelation really harm my client's case? In short, absolutely. There are numerous examples of email being admitted as evidence, for a variety of reasons, because the attorney-client privilege was unintentionally waived.⁵ The facts and details of every case are different, but isn't it easier to safeguard against the possibility of waiver, to the extent possible, in the first place?

But wait, isn't eavesdropping on someone else's communication illegal? In many circumstances it is, under the *Electronic Communications Privacy Act of 1986*.⁶ But even if the sensitive information contained in an unencrypted email doesn't come into evidence as a result, damage could still be done either by a party who uses such knowledge (possibly in a discovery request) without revealing its source, or a nonparty in another context altogether. Unfortunately, it is relatively easy to gain access to unencrypted email without awareness by either the sender or receiver.⁷

³ See generally Legaethics.com, at <http://www.legaethics.com/?s=email> (last visited Aug. 10, 2009) (containing articles that focus "on the ethical issues associated with the use of technology by legal professionals" and bring to the forefront recent ethical technology blunders).

⁴ The client conversation you might be required to have in several of the forty-four states who have adopted data breach security notification laws could be unpleasant. See Privacy & Information Security Law Blog, "New Data Security Breach Laws in Alaska and South Carolina," at <http://www.huntonprivacyblog.com/2009/06/articles/security-breach/new-data-security-breach-laws-in-alaska-and-south-carolina/> (June 26, 2009) (summarizing the most recent legislation regarding data breach notification laws).

⁵ See, e.g., LexisNexis: Redwood Analytics, "Unencrypted Emails Between Attorneys and Clients May Not Be Privileged," at <http://www.lexisnexis.com/Community/redwoodanalytics/blogs/morepartnerincome/archive/2008/02/01/unencrypted-emails-between-attorneys-and-clients-may-not-be-privileged.aspx> (Feb. 1, 2008) (discussing recent cases where courts have found that the attorney-client privilege was waived where confidential information was sent via unencrypted email).

⁶ 18 U.S.C. § 2510, *et seq.*, available at http://www.usdoj.gov/criminal/cybercrime/wiretap2510_2522.htm (last visited Aug. 10, 2009).

⁷ Flaherty, Kristina Horton, "Ethical Issues Bedevil Lawyer Email," California Bar Journal, at <http://www.calbar.ca.gov/calbar/2cbj/01may/page16-1.htm> (reporting that, in one case, it took less than two hours to hack a traditional email account).

III. Introducing the E-Word.

We're talking about "encryption." It may sound complicated, but it's far easier to understand than it first appears. The Greeks and Romans did it for centuries by turning messages into simple code in case they were intercepted. But today, we are in the business of practicing law, not history or information technology, right?

Fair enough, but the modern lawyer can't afford to jeopardize his or her practice by sending important data into the great unknown we call the Internet, without any protection whatsoever. You wouldn't send confidential information through the mail on the back of a postcard, and you shouldn't let sensitive data leave your computer without a secure envelope to protect it.

You might be thinking: "but I encrypt my hard drive" or "I use a firewall." These are all necessary precautions, but consider what happens in the moment you send a traditional email. In short, the "message header" (the information that contains specific data on the sender, receiver, and date) and the "message body" (the text of the email plus any file attachments) are broken into "packets"—which leave your local network and wind their way across multiple computers (stopping at various email servers that re-aggregate the packets to attempt delivery), before they finally wind up reassembled at your intended receiver's inbox.⁸

IV. Getting the Message.

So what's the problem with traditional email? These packets are distributed across the Internet in "unencrypted" plain text, and are readable in plain English by anyone who cares to intercept them. Worse yet, when these packets are re-aggregated at various email servers, the entire message is completely viewable, copyable, and storable, often without your knowledge or consent, for an indeterminable amount of time.⁹

But isn't interception difficult when these packets wind up all over the Internet? Not necessarily. Although packets may choose a variety of routes unknown to you, when

⁸ See EmailIsDangerous.com, at <http://www.emailisdangerous.com/Test.aspx> (last visited Aug. 10, 2009) (providing more information and a visual overview of this process).

⁹ *Id.*

those routes become regularly used, patterns emerge.¹⁰ The problem is that you don't know who would want to sniff your email, and why. It could be your competitor looking for an edge, a hacker gathering information, a foreign entity, or any number of other would-be interceptors—the possibilities are endless.

Should I be worried about telephone calls and postal mail? Maybe a little, but definitely not at the expense of overlooking the far more salient online pitfalls. Without doubt, the traditional wired telephone can be wiretapped, and even though the transition to digital cell phone technology has made eavesdropping on wireless calls more difficult, it is still not impossible. Meanwhile, postal mail can always be misdirected, opened, and read. However, with postal mail, the model is simply A-to-B (sender to receiver), and affirmative physical intervention is required to intercept the communication. Not so with email. In a model where information can instantly travel from A-to-Q-to-G-to-X-to-B, the points of potential interception and retention are numerous.¹¹

What about human error? It happens. You could accidentally hit the wrong button on the fax machine, or simply misaddress an envelope. Chances are good that the ultimate (albeit unintended) recipient would simply tell you that you have the wrong number, repackage your mailing, or throw it in the trash. However, misdirection in a digital world is far more dangerous. Emails can be improperly addressed with the assistance of features like auto-fill, then instantly printed, copied, stored—and worst of all—forwarded, with very little effort whatsoever.¹² Once the message has been sent through various computer locations across the Internet (and stored in a multitude of servers along the way), un-ringing the email bell is often difficult, if not impossible.

V. Piecemeal Solutions to a Multifaceted Problem.

Solutions that address only one weakness of traditional email, like receipt confirmation alone, are insufficient. Receipt confirmation is critical, because you must be able to show that your intended recipient received your message. However, an unfortunate situation may still

¹⁰ See Masur, Joshua M., "Safety In Numbers: Revisiting the Risks to Client Confidences And Attorney-Client Privilege Posed by Internet Electronic Mail," 14:3 Berkeley Tech. L.J. 1117 (Fall 1999), available at <http://www.law.berkeley.edu/journals/btlj/articles/vol14/Masur/html/text.html> (discussing in detail the subject of packetization).

¹¹ See Coon, Karen M., "United States v. Keystone Sanitation Company: E-mail and the Attorney-Client Privilege," 7:3 Rich. J.L. & Tech. 30 (Winter 2001), available at <http://law.richmond.edu/jolt/v7i3/article4.html> (discussing the distinctions between email and traditional communication methods in the practice of law).

¹² See, e.g., Berenson, Alex, "Lilly Considers \$1 Billion Fine to Settle Case," NYTimes.com, at <http://www.nytimes.com/2008/01/31/business/31drug.html?scp=1&sq=zyprexa&st=nyt> (Jan. 31, 2008).

arise when an important document is sent only with a read-receipt, and the entire email is delivered in plain text. Some email solutions today focus predominantly on the read-receipt process, without engaging the real full-message encryption question, by repackaging the message body as an encrypted PDF. This means that the recipient may not be able to easily search or organize the contents of the message as he or she may desire, and the message header is not necessarily encrypted.

So why not use “encrypted” email protected by a methodology like PGP? PGP (or “Pretty Good Privacy”) encryption methods provide a solid means of protecting the email body, but may leave the important message header details unencrypted.¹³ Furthermore, Pretty Good Privacy requires the exchange of keys to lock and unlock messages — which can become confusing to senders and recipients alike. It can be difficult and expensive to deploy and manage, too.¹⁴

What about using another protocol, like FTP, to deliver sensitive files and messages? FTP (or “File Transfer Protocol”) permits the relatively easy uploading and downloading of files across the Internet. However, FTP was not designed specifically for written messages, which would have to be saved in readable file formats, uploaded by the author, and downloaded by the receiver. Furthermore, traditional FTP is not inherently encrypted, so additional steps are necessary to protect the exchange of data across FTP.¹⁵

VI. The Time is Now.

The legal profession can no longer hide behind excuses. The medical profession has HIPAA.¹⁶ Other industries are required to abide by a myriad of consumer data protection laws. Lawyers are in the unique position to act now, and maybe even avoid the imposition of

¹³ See Hopkins, R. Scot & Pamela R. Reynolds, “Redefining Privacy and Security in the Electronic Communication Age: A Lawyer’s Ethical Duty in the Virtual World of the Internet,” 16 Geo J. Legal Ethics 675 (Summer 2003).

¹⁴ See EmailIsDangerous.com, at <http://www.emailisdangerous.com/Research.aspx> (last visited Aug. 10, 2009) (explaining how PGP methodology works).

¹⁵ *Id.*

¹⁶ See Woessner, Ron, “Trust Me — I’m a Doctor (Not a Lawyer): Ethical Standards for Confidential Communications,” Blawgletter, at <http://blawgletter.typepad.com/bbarnett/2009/05/guest-blawg-ron-woessner-and-chris-knowles.html> (May 5, 2009) (comparing the medical profession’s email encryption requirements with the legal profession’s lower standards for email security); Zick, Colin J., “AMA Adopts Principles on EMR Breach,” Security, Privacy and the Law: Legal Perspectives on the Expanding Universe of Information Security & Privacy Issues, at <http://www.securityprivacyandthelaw.com/2009/06/articles/data-breach-1/ama-adopts-principles-on-emr-breach/> (Aug. 6, 2009) (describing what happens in the event of an Electronic Medical Record (EMR) privacy breach).

a mandatory, industry-wide standard which could cramp both the development of new technologies, as well as individual choice to adopt the best platform for one's own practice.

Times are changing. A lot has changed in the world of Internet technology in the decade since the American Bar Association reasoned, in *Formal Opinion 99-413*, that a lawyer may be able to use unencrypted email without violating his or her ethical duty.¹⁷ However, even ten years ago, the ABA acknowledged that this very conclusion does not "...diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure, and the relative security of the contemplated medium of communication."¹⁸ Furthermore, the *Formal Opinion* clarified that "when the lawyer reasonably believes that confidential client information being transmitted is so highly sensitive that extraordinary measures to protect the transmission are warranted, the lawyer should consult the client as to whether another mode of transmission...is warranted."¹⁹

So ask the basic question before sending an email: would my recipient feel comfortable with this information on the back of a postcard? If so, traditional email is certainly appropriate. If not, a more appropriate communication method may need to be considered, as indicated in certain recent publications critiquing *Formal Opinion 99-413* for presupposing that interception of traditional email would not only be illegal (thereby extending certain protection to the confidentiality of its contents), but it would also be difficult, given the packet-based transfer methodology behind Internet email—two assertions which have been drawn into question.²⁰ In any event, even if traditional email is eventually and unequivocally determined to be professionally suitable for certain types of confidential communications, a myriad of pending state and federal laws governing the storage and transmission of sensitive information potentially could

¹⁷ See ABA Formal Opinion 99-413 (Mar. 10, 1999), available at <http://www.abanet.org/cpr/pubs/fo99-413.html>.

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ Masur, Joshua M., "Safety In Numbers: Revisiting the Risks to Client Confidences And Attorney-Client Privilege Posed by Internet Electronic Mail," 14:3 Berkeley Tech. L.J. 1117 (Fall 1999), available at <http://www.law.berkeley.edu/journals/btlj/articles/vol14/Masur/html/text.html>.

be triggered by failing to encrypt certain types of data contained therein.²¹ All of this is not to mention that the disclosure of confidential communications—even where “ethical”—can present a host of other serious repercussions for everyone involved.

Legislation aside, attorneys should do what is best for their clients. We owe our clients an express ethical obligation to “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...”²² Regardless of the question of whether we could unintentionally waive confidentiality, our clients’ data is important—period. With the ever-increasing number of newsworthy security breaches, individual attorneys (and the profession as a whole) must not delay in securing the online transmission of sensitive client materials whenever possible.

What does my jurisdiction require? Recommendations and requirements vary from state to state, so you should review your local guidelines carefully. A common theme in those jurisdictions expressly permitting communication in all cases by traditional email arises with respect to suggested (and sometimes mandatory) client notification and consent when confidential correspondence is to be delivered by unencrypted means.²³

²¹ The FTC’s “Red Flag” Requirements, which are anticipated to be effective on November 2009, apply specifically to financial institutions. See Federal Trade Commission, FTC Business Alert, “New ‘Red Flag’ Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft,” at <http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm> (June 2008). But additional state-by-state rules and regulations have been, and continue to be, adopted and debated. See, e.g., Nevada, Nev. Rev. Stat. § 597.970, available at <http://www.leg.state.nv.us/Nrs/NRS-597.html> (last visited Aug. 10, 2009) (“A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.”); Massachusetts, 201 CMR § 17.00, available at <http://www.mass.gov/?pageID=ocaterminal&L=4&L0=Home&L1=Consumer&L2=Privacy&L3=Identity+Theft&sid=Eoca&b=terminalcontent&f=reg201cmr17&csid=Eoca#1703> (last visited Aug. 10, 2009) (“Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information.”). For additional information regarding the FTC’s “Red Flag” Requirements, see Helmer, Gabriel M., “FTC Issues Guidance to Businesses on How To Handle Social Security Numbers,” Security, Privacy and the Law: Legal Perspectives on the Expanding Universe of Information Security & Privacy Issues, at <http://www.securityprivacyandthelaw.com/2009/01/articles/identity-theft-1/ftc-issues-guidance-to-businesses-on-how-to-handle-social-security-numbers/> (Jan. 15, 2009).

²² ABA Model R. Prof. Conduct 1.6(a), available at http://www.abanet.org/cpr/mrpc/rule_1_6.html (last visited Aug. 10, 2009).

²³ See generally American Bar Association, Legal Ethics and Technology: Confidentiality, at <http://www.abanet.org/tech/ltrc/research/ethics/confidentiality.html> (last visited Aug. 10, 2009).

Modern legal correspondence requires a comprehensive solution. We have just discussed two competing realities: (1) encryption of sensitive material, although necessary, can be complicated to employ due to the piecemeal nature of many available solutions; and (2) we as attorneys can no longer delay adoption of secure communication technologies. But what if a comprehensive, encrypted communication platform, specifically for lawyers, was both simple to use and available now? The answer is clear—we would simply do it—if not out of proactive dedication to the welfare of our clients’ data, then out of concern for the consequences of failing to act when our competitors are doing so, lest we appear negligent in the process.

VI. SSL: The Key to Securing A Comprehensive Platform.

Solutions are emerging, but you have to be selective. As always, some answers are better than others. As we have discussed, many solutions fall short because they are too difficult to implement, or because they only address certain facets of the encryption-transmission process. Others may be inadequate because they only cater to one set of communication needs, such as working well for files but not email, failing to work across multiple platforms (Mac® / PC) or multiple devices (iPhone® / Blackberry®), or completely ignoring the need to communicate verbally when necessary (via integrated voicemail). Finally, many solutions are just too expensive, as they base charges upon the number of messages sent or files shared.

A unified platform will bring everything together under one encrypted umbrella. SSL, or “secure socket layer” technology, provides encryption for the packets traveling between you and your recipient. This virtual pipeline can deliver just about any digital information you like—from text to complex files—with very little maintenance when properly deployed.²⁴ Of course, the encryption is only as good as the entity maintaining the necessary “certificates” used to verify the connection, and the service provider selected to incorporate those certificates into the overall platform.

No matter what, keep it simple. The more simple the integration, the easier it is to deploy and maintain. In fact, some solutions are so simple that they are *entirely* hosted online—or in the “cloud”—meaning that there is no software to install, and everything is automatically backed up in an offsite location. With such a solution, you can spend less time thinking about your information technology and more time concerned about your clients’ needs. After all, isn’t that what the practice of law is really all about?

²⁴ See EmailIsDangerous.com, at <http://www.emailisdangerous.com/Research.aspx> (last visited Aug. 10, 2009) (explaining how SSL encryption works).