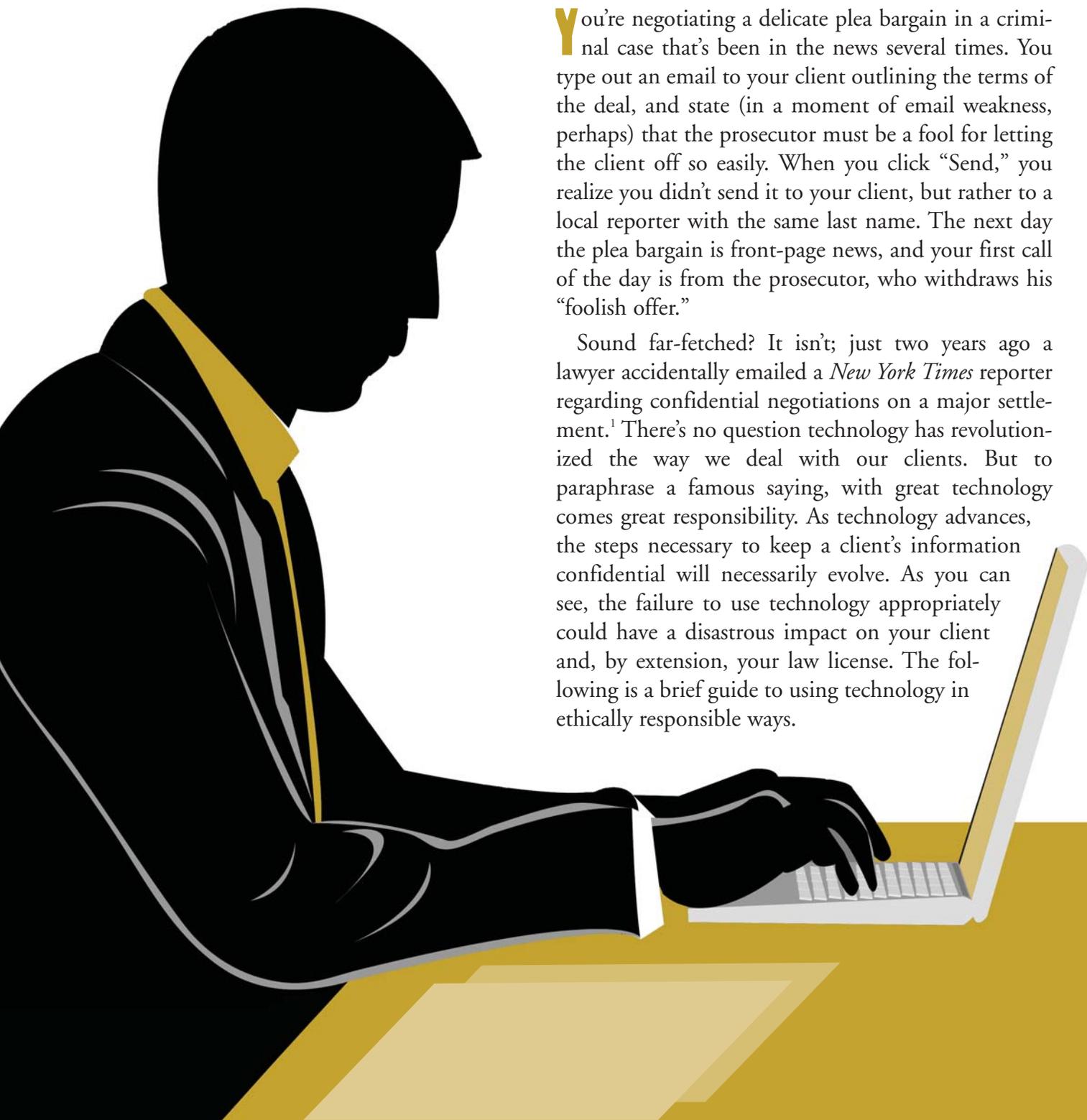


THE CYBER-ETHICAL CRIMINAL DEFENSE LAWYER (OR, HOW NOT TO COMMIT MALPRACTICE WITH YOUR TECHNOLOGY)

BY TOM MIGHELL

You're negotiating a delicate plea bargain in a criminal case that's been in the news several times. You type out an email to your client outlining the terms of the deal, and state (in a moment of email weakness, perhaps) that the prosecutor must be a fool for letting the client off so easily. When you click "Send," you realize you didn't send it to your client, but rather to a local reporter with the same last name. The next day the plea bargain is front-page news, and your first call of the day is from the prosecutor, who withdraws his "foolish offer."

Sound far-fetched? It isn't; just two years ago a lawyer accidentally emailed a *New York Times* reporter regarding confidential negotiations on a major settlement.¹ There's no question technology has revolutionized the way we deal with our clients. But to paraphrase a famous saying, with great technology comes great responsibility. As technology advances, the steps necessary to keep a client's information confidential will necessarily evolve. As you can see, the failure to use technology appropriately could have a disastrous impact on your client and, by extension, your law license. The following is a brief guide to using technology in ethically responsible ways.



But first, let's consider the case for why a basic understanding of technology is important for lawyers. It starts with Rule 1.01 of the Texas Disciplinary Rules of Professional Conduct, the "Duty of Competence."² Should this duty extend to an understanding of technology? The lawyers in Maine think so:

[W]e also do not believe it reasonable for an attorney today to be ignorant of the standard features and capabilities of word processing and other software used by that attorney. ...³

The Canadian Bar Association agrees:

Lawyers must be able to recognize when the use of a technology may be necessary to perform a legal service on the client's behalf, and must use the technology responsibly and ethically.⁴

Such rules have not yet spread to Texas or most other parts of the country. But it's not hard to imagine the day when courts and grievance committees nationwide will be considering such issues. It is difficult these days to provide competent representation to clients *without* the use of technology; lawyers must recognize this fact and be prepared.

Other ethical rules have implications with technology (Conflicts of Interest, TDRPC Rules 1.06–1.09; Diligent Representa-

tion, TDRPC Rule 1.01), but for purposes of this article, the most important is TDRPC 1.05, the Duty of Confidentiality. The rule applies to any communication of client information — verbal, written, or electronic. It applies to both intentional and accidental disclosures of such information, not only to the attorney but also the rest of the law office staff. From a technology standpoint, this rule deals with communications between a lawyer and client as well as the steps a lawyer takes to protect the client's confidential information residing on the firm's computer systems. Let's start with the tool used more than ever these days to communicate with clients: email.

EMAIL AND PRIVILEGED COMMUNICATIONS

More than 93 percent of lawyers send confidential or privileged communications to clients through email during the course of a year.⁵ Although most email reaches its intended destination, some messages go astray. Who's to blame for this? While it's true that hackers may be out there intercepting emails right and left, the fact is most email confidentiality is compromised by *user error*. Here are just a few ways that it can happen:

- Misdirected communications by sending to the wrong address;
- Sending to the correct address, but attaching another client's document;



You already have a complete digital dictation system in your pocket.

SpeakWrite is now available on iPhone and Blackberry

- Turn your phone into a digital office with our US based transcriptionists
- You can record dictation of any length from anywhere with full editing capabilities
- You can record telephone calls, meetings or interviews for transcription
- Or take photos and integrate those into your dictation
- And with our 24/7 transcription staff, your completed work is delivered to your email and your mobile device in about 3 hours
- The App is free; you simply pay for the work transcribed and nothing else

(800) 828-3889

www.speakwrite.com/TXBJ

SPEAKWRITE
Voice-To-Document Service

- Interception of the email by the system administrator (often on instructions of the employer) once it enters the recipient's network; and
- Compromise of the attorney's email password (which is usually kept on a sticky note attached to the lawyer's monitor).

In other words, lawyers can avoid many inadvertent disclosures of confidential email by paying better attention to the process of sending, receiving, and storing email.

PROTECTING EMAIL AGAINST DISCLOSURE

Based on the state of the law on email and confidentiality, you might expect that most attorneys do little or nothing to protect their email communications. And you'd be right. In the 2009 American Bar Association Technology Survey, only 8.4 percent of respondents do nothing to secure their emails. However, a whopping 85 percent rely on a simple confidentiality statement contained within the message. What's wrong with a disclaimer, you ask?

- Using a form notice arguably is circumstantial evidence that the sender knew the email was insecure;
- It also could be direct evidence the sender knew email to be insecure and chose to try to protect it by an ineffective method (disclaimer) instead of an effective one (encryption);
- The disclaimer is often placed at the end of the email, so the unintended recipient has already read the privileged content by the time he or she gets to the warning; and
- A prospective (but not retained) client of the firm who receives such a disclaimer may assume that the language creates an attorney-client relationship.

Lawyers who choose to add additional protections to their emails usually do so by means of encryption or a digital signature. Although these options are not required, they demonstrate that reasonable measures are being taken to protect against the inadvertent disclosure of confidential information.

TIPS FOR MORE SECURE EMAILING

As noted above, many email disclosures occur when the sender does not exercise appropriate precautions before sending an email. Here are a few tips to help you become a more secure emailer:

- Avoid sending email to the client's place of employment (unless the client is self-employed). Most employers have email use policies that reserve the right to intercept and review all communications passing through their networks. If you must send email to the client's work address, obtain express written permission first.
- Regardless of where you send email to a client, consult the client first and consider obtaining the client's permission to communicate via email in the retainer agreement before beginning the representation.

- Always draft an email as if it were a discoverable document. Because in many cases, it is.
- Write in clear, direct, and concise language.
- Appropriate addressing of email:
 - ◆ Don't send email to opposing counsel and BCC your client just to save time.
 - ◆ When you want to reply to an email sent to multiple recipients, don't "Reply to All" unless you want everyone else to know what you're saying; and
 - ◆ Take care when forwarding a document — you may be unintentionally forwarding confidential information to the wrong person.

PROTECTING CLIENT DATA IN OTHER WAYS

Here are a number of things to think about when protecting client information that resides on your computer servers, laptops, smartphones, or other electronic media.

Protection from Outside Attack

You are probably thinking, "Who would want to hack into my computer?" And that's generally correct; typically, the average hacker probably has no real interest in the information on your computer. Historically, however, solo and small firm lawyers have been subject to attack from outside, for one simple reason: Outdated operating system software. It's a fact that Windows operating software has many flaws and weaknesses — nearly every week Microsoft sends out new fixes on "Patch Tuesday." The hackers know this and try to exploit the weaknesses on unpatched computers. Often, solo and small-firm lawyers are still using earlier versions of Windows and are not diligent about updating them on a regular basis. What can you do to avoid becoming the target of hackers or of other computer ills?

- **Windows Update.** Run Windows Update regularly to download and install software patches from Microsoft. You can configure Windows Update to automatically download critical updates as they are released.
- **Firewall.** You likely already have a firewall — make sure it's up-to-date and always on. Hackers can break into an unprotected computer in seconds — really.
- **Anti-Virus Software.** You likely also have anti-virus software; however, you may not be keeping your antivirus definitions up to date. New viruses appear every day, and your best defense against these destructive bugs is to maintain the most current protection.
- **Spyware/Malware Detection.** Any law firm employees who use the Internet at work are likely to have some trace of spyware on their computers. Most spyware is relatively harmless, intended only to monitor your Internet activity for marketing purposes. However, some types of malware can not only steal your confidential information, they can cause damage to your computer system. To protect against spyware, download and run a spyware-removal tool at least once a month.

DANGERS WITHIN YOUR FIRM

Not all disclosure of firm information comes about as the result of an insecure computer system. In fact, many problems occur due to careless or even malevolent conduct by firm employees. Ways in which this can happen include:

- **Sending Large Attachments via Email.** This can clog up the firm's email server, create a slowdown in the delivery of email, and potentially crash a network. Use a program like YouSendIt or Drop.io to transmit large files to others.
- **Downloading of Inappropriate Material.** As a rule, it's okay to use the Internet at work for personal reasons, but only on a limited basis. Employees must be educated in the safe operation of their computers, so they do not inadvertently download a virus, Trojan horse, or spyware product.
- **Forwarding Firm Information to Others.** Employees who are either disgruntled or planning a change in employment may attempt to send firm information outside of the organization. This information is often proprietary in nature, and may contain confidential communications regarding clients of the firm.

To protect against these risks, a law firm should have an Internet and electronic communications policy notifying all employees that 1) inappropriate use of the Internet is not permitted and 2) firm management has the right to monitor email communications and Internet activity for any reason, and that employees should have no expectation of privacy in any activity taking place on office computers and networks.

METADATA

Another way confidential information can be disclosed is through the inadvertent release of metadata. The official, unhelpful definition of metadata is "data about data." A better definition is "data associated with a document, but not visible in the ordinary display of the document." More simply put, metadata is information contained within an electronic file that is there to help revise, organize, and access the file. Some important types of metadata include the date a file was created, modified or printed, the previous authors of a document, revisions to a file, and comments made by authors. Probably the best-known form of metadata or embedded data is found in the track changes feature of Microsoft Word. Lawyers frequently use track changes to work on documents with others. If not handled appropriately, tracked comments and revisions can remain with a document, even when it may appear that they no longer exist. The problem is not limited to Microsoft products, either. Nearly every file created on your computer contains some form of metadata.

Being aware of the types of data that can travel with a document is the first step in dealing with metadata. Getting rid of it (under the proper circumstances) is the next. There are several ways to remove metadata from documents. The most effective is a metadata removal application, and Payne Consulting's Metadata Assistant is one of the best. Metadata Assistant ana-

lyzes your document, shows the metadata contained within it, and safely and easily removes it. You can also run the program on a batch of documents, cleaning all of them at once.

Another way to remove metadata from a document is to convert it to PDF. Adobe Acrobat or other PDF-conversion programs will remove most of the metadata in a file. While converting a file to PDF is one of the better ways to remove metadata, it is not a useful option if you want the recipient of your document to be able to edit it. That's why a metadata removal tool is still your best bet. Another way to remove most of your Word file's metadata is to convert it from .doc format to .rtf (rich text format). This will remove tracked changes and comments from a document.

BACK UP YOUR SYSTEM

Even if you take all of the precautions described above, they will be for naught if you fail to routinely back up your data. The method of backup will depend on your computer network configuration and the size of your firm. Different methods of backup include tape, stand-alone hard drives, and even CDs and USB drives for small amounts of data. Lately, online backup has become a popular alternative, with services like Mozy and Carbonite offering low-cost, high volume storage. Store your physical backups offsite and perform a full test restore regularly to make sure you can get your data back. And don't forget to back up the information on smartphones and laptops; often they are neglected because they are not always attached to your computers. Having both a physical backup as well as an online duplicate is a good way to ensure your client information is safe in the event of a disaster or other business interruption.

Choosing to trust an online backup provider to store confidential client data can be difficult for a lawyer. Make sure you are satisfied with the answers to these questions before taking the online plunge:

- Where will the data be kept?
- What is the company's security? (Most backup security is ten times better than yours, but it's worth asking.)
- How is the backup data transmitted?
- What happens if I don't pay my bills?
- What happens if your company goes out of business?
- What happens if your servers crash? and
- If I lose my data, how do I restore it?

PHYSICAL SECURITY OF CLIENT DATA

You can also compromise a client's confidences simply by allowing physical access to the data that's being protected. Here are a few things to think about.

Non-Mobile Hardware

Does your receptionist have a computer at her desk? If so, is the information on that computer protected if she happens to be away from her desk? Can someone walk into your firm's lobby and use the unattended PC without anyone noticing? At a minimum, password-protect any firm computers that can

possibly be accessed by the public. Even better, don't even connect these publicly accessible computers to the firm's network.

Mobile Technology and Security

Hundreds of laptops are stolen (or more likely, lost) every single day. If your laptop falls into the wrong hands, is it sufficiently protected? Laptops should be password-protected, and consider encrypting or assigning passwords to individual folders or files. Some law firms make use of LoJack for Laptops services that send a signal back to the owner when a stolen laptop is connected to the Internet. Some of these services also have the ability to remotely wipe a computer hard drive clean, once an Internet connection is established.

Handheld Security

The same holds true for your BlackBerry, iPhone, or other handheld device. Protect access with a password, and consider disabling Bluetooth or wireless capabilities when you aren't using them. Some phones also come with software that automatically erases the data after a certain number of incorrect password entries.

WIRELESS SECURITY AND USING THE INTERNET

Access to and use of the Internet is probably the biggest headache for the security-minded lawyer on the road. And with wireless access nearly ubiquitous, safe computing is even more important; wireless technology is just not completely secure — yet. Here are some tips to make sure your wireless Internet experience doesn't attract hackers or the like.

A Real Connection

First, make sure you're really connected to the legitimate access point. Believe it or not, the bad folks can create "rogue" access points that fool you into believing they are real; it's only after you have given up your credit card information that you realize you've been duped. Don't configure your laptop to automatically connect to any available network.

Disable Print and File-sharing

There's a setting in Windows that allows you to share and print files with other computers on a network. However, this feature also provides a gateway for anyone wanting easy access to your laptop. Make sure you disable this functionality if you're out on the road.

- **Consider Encryption.** While data that you send and receive from secure web sites (those beginning with https:) is generally protected, information sent through other sites can be intercepted easily by someone nearby using something called a "packet sniffer." Think about using a program (for example, Pretty Good Privacy) that will encrypt your emails and attachments.
- **Use a VPN.** A VPN (Virtual Private Network) is software that basically creates a private network through a public network via a "tunnel" between the two endpoints, which generally cannot be hacked.

Using a Public PC

One word of advice when using public computers to access email or work files: *don't*. It's just not safe to use a system with which you are not familiar. But if you must use a computer at an Internet cafe, library, or airport, follow these basic rules:

- **Be Aware.** Look around to make sure no one is looking at your screen or keyboard while you're typing.
- **Watch Out for Keyloggers.** Hackers may install "keylogging" programs that can capture your keystrokes — and therefore your passwords, credit card numbers, or anything else you type on a keyboard. There are two ways to get around this. First, use the onscreen keyboard to enter passwords with your mouse. Just select Start, then Accessories, then Accessibility, then On Screen Keyboard. Another way to enter passwords is to type your password with a lot of other letters/numbers in the middle, then remove those items with your mouse.
- **Erase Your History.** If you use a browser on a public computer, make sure that you clear your browsing history before you go.
- **To-Go Software.** Better yet, use a browser, word processor, and password manager that leave no trace of your computer activity when you're done. Carry a copy of Portable Apps or Pass2Go on a USB drive; you can surf the Internet, edit documents, and fill in forms securely. When you unplug your USB drive from the public PC, all traces of your activity go with you.

This article merely skims the surface of the issues lawyers must consider when using technology to serve their clients. Lawyers are opening "virtual" law practice in increasing numbers, and are using social networking tools like LinkedIn, Facebook, and Twitter to interact with clients and colleagues. Understanding the technology you use in your practice will not only allow you to provide more efficient, potentially more economical service to clients, it may also keep you out of trouble. And that's a win-win for you and your clients.

NOTES

1. *Did Lawyer's E-Mail Goof Land \$1B Settlement on NYT's Front Page?*, ABA Journal Online, Feb. 6, 2008, http://www.abajournal.com/news/article/lawyers_e_mail_goof_lands_on_nyts_front_page/
2. "A lawyer shall not accept or continue employment in a legal matter which the lawyer knows or should know is beyond the lawyer's competence ..." Tex. Disc. R. Prof. C. 1.01, Competent and Diligent Representation.
3. Maine Ethics Opinion No. 196 (October 2008).
4. "Guidelines for Practicing Ethically with New Information Technologies," Canadian Bar Association, September 2008.
5. American Bar Association Legal Technology Survey Report, Web and Communication Technology, Volume IV (2009).

TOM MIGHELL

is a records management and e-discovery consultant with Contoural, Inc. He currently serves as chair-elect of the American Bar Association's Law Practice Management Section.