



ILLINOIS STATE
BAR ASSOCIATION

STANDING COMMITTEE ON LEGAL TECHNOLOGY

The newsletter of the ISBA's Standing Committee on Legal Technology

From the Chair

By Trent L. Bush

Welcome! It is my pleasure to serve as the Chair of this year's Committee on Legal Technology (COLT). We have a fine committee with members of diverse backgrounds—lawyers and non-lawyers, practitioners and non-practitioners, techies and traditionalists, etc. We believe you will find this newsletter to be a useful (and perhaps even entertaining) resource for tech related issues.

What is COLT? For those that are new to COLT (or even for those of us who have been around for a while), I think it is helpful to review COLT's mission statement:

The mission of ISBA Standing Committee on Legal Technology

- to advise ISBA members on the implementation of technology in their law practices;
- to advise other ISBA section and committees on proposed projects;
- to advise other legal entities on the development of programs and systems to better circulate information to the public and expedite the prac-

tice of law on all levels;

- to develop a communications network for use of ISBA members, with membership on the system available upon membership in the ISBA;
- to serve as a clearinghouse for technical information; and
- to serve as a liaison between the ISBA and other bar associations, as well as non-legal entities which address technology issues.

In short, we're here to help the ISBA as an organization and you as a practitioner with tech issues.

COLT's Priorities. To that end, we have established the three short and near-term priorities.

1. Electronic Courts in Illinois.

First, COLT will focus on the issue of electronic courts in Illinois. We want to educate the membership on the status of electronic courts in Illinois, particularly after the pronouncement on the issue by the Supreme Court in May (see <http://www.state.il.us/court/media/PressRel/2008/052308.pdf>). We intend to explore (1) where Illinois is at regarding electronic courts; (2) the issues (technological, fiscal, political, etc.) surrounding the concept; (3) where others are at (other states in particular); and (4) where we might be headed. We will be a resource to the ISBA directly and to our membership indirectly by being part of the conversation.

2. Tech for Lawyers.

Second, COLT will be a visible and accessible resource for day-to-day tech issues in our practices. To increase our impact, we intend to (1) expand our

AskCOLT question / answer feature to increase its presence and effectiveness in responding to inquiries; and (2) present a CLE program focused on the tech issues of interest and benefit to our members' practices.

3. Resource to the ISBA.

Finally, COLT will be a valuable resource to the ISBA itself. We will strive to be utilized for tech issues that will increase the reach and value of the ISBA to its members. In particular, we will assist efforts such as playing a leading role in the Solo & Small firm conference, providing input and assistance in redesigning the ISBA's Web site, and developing more effective ways to perform committee functions, such as legislative review.

Closing Remarks. Before signing off, I want to give special recognition to two individuals who have made standout contributions to COLT over the past year. The first is David Yavitz, who completed his second (at least) tour of duty as Chair. David's technical expertise, legal experience, and passion (particularly when it comes to Mac products) have contributed greatly to our Committee and the ISBA. The second is Bryan Sims, who has served as our newsletter editor for the past several years. Bryan has managed to tame what has traditionally been the unwieldy beast that is our newsletter and produced many fine issues. Bryan has graciously agreed to accept the lead role once again this year. Thanks to both David and Bryan.

Stay tuned—we think you'll like what you're going to see. We look for-

IN THIS ISSUE

- From the Chair 1
- Intersection of technology and your job search—Techniques to streamline and stand out 2
- E-mail encryption 3
- Bill4Time Internet-based time and billing software 6

ward to serving you.

Trent L. Bush
Ward, Murray, Pace & Johnson, P.C.
202 E. Fifth St.
P.O. Box 400

Sterling, IL 61081
ph: 815.625.8200
fax: 815.625.8363
Web: www.wmpj.com
E-mail: bush@wmpj.com

Intersection of technology and your job search – Techniques to streamline and stand out

By Jennifer Bertoglio, Esq., LawyerLink LLC

Just 10 years ago, when the average attorney embarked upon a job search, we would rely on our law school career services office for a list of jobs or pick up a copy of the local newspaper and browse the classified ads. Today, rather than paging through the classified ads and sending out cover letters with resumes, we navigate our way through pages of legal job postings on the Internet. An attorney on the job hunt can now search and apply for a job anywhere in the world in just a few clicks of a mouse. As a result, in this age of electronic resumes and digital job postings, making effective use of technology requires sophisticated strategies to streamline your search and stand out to prospective employers.

Below are a few tips to inject success into your cyber job-hunt:

1. Streamline the information pertinent to your legal job search

Legal job boards are indispensable, numerous, and will publish hundreds of searchable job postings for free. However, without a plan, this can often be an overwhelming process, particularly for attorneys who already are short on time and need to account for every minute of their billing day. One major advantage of using these boards is the e-mail notification you can receive when new postings from firms or corporate legal departments appear that meet your specified criteria. You can typically request to have these postings e-mailed to you on a daily, weekly or monthly basis. Similarly, experienced attorneys looking to transition to another practice area or re-tool their resumes

can analyze the frequency and patterns of legal posts to determine where legal hiring trends occur.

Alternatively, if your inbox is already overflowing, bypass the e-mail notifications and subscribe to an RSS feed. For those who are unfamiliar with RSS, it is essentially a tool for delivering updates of Web-based content. You will most likely need to execute a search on the job board specifying various criteria before one of the following RSS icons will appear somewhere on the page: or. You can subscribe to the feed by entering the feed's link into the reader or by clicking on the RSS icon in a browser that initiates the subscription process. Because the RSS offers instant, real-time distribution, the majority of RSS feeds are used for news headlines or breaking information. A growing number of employers and job boards are now using this new technology to provide job seekers with the latest job postings instantly. For example, Lawjobs.com and Monster.com are two sites where legal jobs are bountiful and RSS feed is an option. The RSS feed is also a great monitoring tool to stay abreast of your client's business or find an area of need that you might address as a job candidate.

For the actively employed attorney conducting an online job search, keep your location in mind as you likely do not want your job search results dumping into your Outlook inbox at work. Similarly, use caution when setting up a profile or posting your resume on a legal job board as current employers might have active searches or feeds on their company names to determine if

Legal Technology

Published at least four times per year.

Annual subscription rate for ISBA members: \$20.

To subscribe, visit www.isba.org or call (217)525-1760

Office

Illinois Bar Center
424 S. 2nd Street
Springfield, IL 62701
Phones: (217) 525-1760
OR 800-252-8908

Web site: www.isba.org

Editor

Bryan M. Sims
1001 E. Chicago Ave., #111
Naperville, IL 60540

Managing Editor/Production

Katie Underwood
kunderwood@isba.org

Standing Committee on Legal Technology

Trent L. Bush, Chair
Bryan M. Sims, Vice-Chair
Adam C. Nelson, Secretary
David Yavitz, Ex-Officio
Aaron W. Brooks
David M. Clark
John A. Coladarci
Robert J. Connor
Todd H. Flaming
Roger H. Gustafson
Stephen F. Hedinger
Peter M. LaSorsa
James A. McKenna
Peter V. Mierzwa
Nerino J. Petro
Alan R. Press
Martin W. Typer
Carl R. Draper, Board Liaison
Steven L. Dunn, Staff Liaison
Paul A. Osborn, CLE Liaison

Disclaimer: This newsletter is for subscribers' personal use only; redistribution is prohibited. Copyright Illinois State Bar Association. Statements or expressions of opinion appearing herein are those of the authors and not necessarily those of the Association or Editors, and likewise the publication of any advertisement is not to be construed as an endorsement of the product or service offered unless it is specifically stated in the ad that there is such approval or endorsement.

Articles are prepared as an educational service to members of ISBA. They should not be relied upon as a substitute for individual legal research.

The articles in this newsletter are not intended to be used and may not be relied on for penalty avoidance.

Postmaster: Please send address changes to the Illinois State Bar Association, 424 S. 2nd St., Springfield, IL 62701-1779.

any employees are actively looking for a new job.

2. Stand out through succinct professionalism and on-point experience

Marketing yourself professionally and succinctly is essential to distinguish yourself in a positive way over the other thousands of legal job applicants competing for your potential job. While you're researching your ideal job, check employers' Web sites to see if they accept online resume submissions. If they do, submit a tailored resume to include specific items such as successful verdicts, motions, transactions, etc. that are directly responsive to the job for which you are applying. In fact, in many instances of online submissions, particularly for larger companies, your resume will be downloaded into a filtering tool utilized by the HR department to determine how closely your resume matches the job description. Therefore, you may be screened out by technology if your experience is not

articulated on your resume.

Similarly, reach out to staffing firms by applying on their Web sites. A staffing firm uses similar screening technology for applicants when they are conducting searches on behalf of their clients; however, they typically are able to conduct a bit broader search, accepting more candidates, as they have several ongoing searches at any one time. Therefore, you may be able to obtain an in-person interview and depending on your experience, the success of your interview, and your interest area, the staffing firm can be a source to connect you with firms and corporations of all sizes in your area.

3. Utilize networking sites to post what you want potential employers to see

Despite all of the efficiencies the Internet offers your job search, there are pitfalls associated with the Internet that job seekers, particularly legal professionals, need to consider as your digital footprint remains for future employers

to see. For example, hiring managers are performing background research on applicants using social networking sites like Facebook or MySpace, professional networking sites such as LinkedIn, and Google research. Sometimes managers have chosen not to hire an applicant after viewing their online profile.

For attorneys, LinkedIn is one favorable forum to be socially active on the Web, but in a professional manner. At the same time, you are networking to meet potential employers and business contacts. By including up-to-date, professional, factual information about your experience and achievements, you may stand out to an employer, perhaps even when you are not expecting it.

About the Author: Jennifer Bertoglio, an attorney and President & CEO of LawyerLink, founded the legal staffing firm in 2005 and specializes in e-discovery, recently building an unprecedented 90-station dedicated review facility in downtown Chicago. More information about Ms. Bertoglio and LawyerLink is available at www.lawyerlinksolutions.com or by calling (312) 962-5750.

E-mail encryption

By Benjamin Gerber and Adam Nelson

Last year in this publication we advocated that you consider strengthening your firm's information security practices and provided a list of practices to follow ("Information Security for the Solo and Small Firm Attorney," June 2007). Among the desired security mechanisms mentioned were Whole-Disk Hard-Disk Encryption and File Level Encryption.

In this article, we will look at another use for cryptography in your everyday activities, encryption of communications, specifically of e-mail and e-mail attachments. We will then explain how to get started using encryption features in two of the most popular e-mail clients, Outlook and Thunderbird.

Why

E-mail encryption features provide confidentiality and integrity for message content and authentication of and

non-repudiation for senders. This can be useful when communication with your client and/or opposing counsel. Most of what we do is confidential and encryption will ensure that the messages remain so. Below we will focus on the need for confidentiality features.

Unless both the sender and receiver are on the same internal office mail server, e-mail messages transverse the Internet in plaintext. In this respect, e-mail is often likened to communicating via postcards, except all the intermediate carriers (servers) and the space between them is not governed by the post office. In addition to messages being stored at the receiving location, and often the sending location, they may also be cached along the way.

While attorney-client privilege limits the use of information shared between you, your clients and external parties for other legitimate purposes, the attorneys' obligation to protect sensitive and per-

sonal data goes beyond this. Whether or not you fall under the purview of privacy regulations that require a higher level of due diligence in protecting personal and sensitive data, measures you take to do so will differentiate you to your clients as an attorney they can trust with their sensitive information. This may also be beneficial to the court. Through the use of encryption you can establish a high level of care.

For e-mail exchanges not covered by privilege, but intended to be private, are messages truly private if we do not take decent measures to protect them? Are we giving up the right to consider messages private at all? Certainly if communicating via postcard or by posting signs in your front yard remove the expectation of private communication, might this be said of e-mail sent in plaintext?¹

Without encryption, e-mail communications can be read by:

- Your e-mail hosting provider,

- including all system administrators and possibly even vendors transporting or holding backup tapes
- Anyone involved in the infrastructure between the origin and destination servers (relay servers and networks)
- The receiver's hosting provider (perhaps it is Google's Gmail which also scans message content to display applicable ads)

Password protected files

We have noticed a trend in the increase of legal practitioners utilizing password protection mechanisms when sending documents via e-mail. While this demonstrates awareness of the risks and an effort to mitigate them, it must be noted that many file password protection mechanisms offer no real security and can be overcome by opening files with applications that do not support the password mechanism, or the passwords can be removed or recovered using easy to use utilities. (Proper encryption options for files will be covered in a later article).

Encrypting e-mail passwords

TLS (Transport Layer Security) and its predecessor SSL (Secure Sockets Layer) is the same technology that allows us to encrypt data sent via a Web browser (such as when you log into your bank's Web site), and provides us with the ability to secure our IMAP or POP e-mail when it is retrieved from and sent to our mail server. This will not protect mail sent to users on other mail servers or the messages stored on a mail server; however, it does protect your password used to receive and send mail from being transmitted across your network and the Internet in plaintext.

TLS and SSL are often used for point to point encryption. Point to point encryption solutions address the encryption of data on or in between systems; the data is unencrypted (and optionally re-encrypted) whenever it reaches or leaves systems throughout an architecture.

In order to use this option, TLS or SSL must be supported by your e-mail hosting provider. If you are using an IMAP or POP e-mail account, the following instructions can be used.

Thunderbird

- 1.) From the top menu select 'Tools' → 'Account Settings' (on some platforms: 'Edit' → 'Account Settings')

- 2.) Select 'Server Settings' for your account
3. Select 'TLS' or 'SSL' under 'Security Settings' → 'Use secure connection:' (for IMAP, the default port will automatically change to 993)
4. Select 'Outgoing Server (SMTP)' from the 'Account Settings' list
5. Click 'Edit' for your SMTP server
6. Select 'TLS' or 'SSL' under 'Security and Authentication' → 'Use secure connection:' (the default port will automatically change to 465)
7. Click 'OK' for 'SMTP Server' settings
8. Click 'OK' for 'Account Settings'

Outlook

1. From the top menu select 'Tools' → 'E-mail Accounts'
2. Select 'View or change existing e-mail accounts'
3. Click 'Change' for your account
4. Click 'More Settings'
5. Click on the 'Advanced' tab
6. Under 'Incoming server,' check 'This server requires an encrypted connection (SSL)' (for IMAP, the port will automatically change to 993)
7. Under 'Outgoing server,' check 'This server requires an encrypted connection (SSL)' (the port will NOT automatically change; depending on your hosting providers configuration, you may need to change this port number, e.g. from 25 to 465)
8. Click 'OK' for 'Internet E-mail Settings'
9. Click 'Next' for "E-mail Accounts" settings
10. Click 'Finish' for "E-mail Accounts" settings

Encrypting e-mail content

There are two prevalent and standardized implementations of e-mail encryption. Both of these options provide message level security. The major advantage message level encryption provides is an end-to-end security context – as the message flows from system to system it remains encrypted.

Whichever option you select may depend on what others you communicate with on a regular basis are using, since both parties must be utilizing the same standard to exchange encrypted e-mail. If you have diverse correspondents, you can use both. Both S/MIME and OpenPGP require exchanging public keys (for S/MIME the public key is contained in a certificate); you must send your public key to those who will

send you encrypted messages and you must have your correspondents' public keys before sending them encrypted messages. It is possible to automate this key exchange, as we will explain below for S/MIME configuration.

Below we will refer to "signing" and "encrypting" a message. Signing adds a signature to the message, providing a level of assurance that it came from you and that it was not modified after you sent it. Encrypting a message prevents the message from being read by anyone other than the intended recipients. Messages can be signed or encrypted, or both signed and encrypted.

S/MIME

S/MIME (Secure MIME; MIME, Multipurpose Internet Mail Extensions, is how e-mail clients exchange non-text portions of messages) is built in to many e-mail clients (including Outlook and Thunderbird). Because it does not require installing and supporting additional software it is often the choice of many large organizations.

To get started w/ S/MIME, you will first need a digital certificate, your organization or firm may have their own certificate authority (CA), or you can obtain one from a third party certificate authority, such as Thawte (<http://www.thawte.com/secure-email/personal-email-certificates/>) or CAcert (<http://www.cacert.org>).

It is common practice to use separate certificates for signing and encrypting messages in large organizations. This allows for the encryption certificate to be kept in escrow without compromising the integrity and non-repudiation achieved when signing messages with a certificate only in the sender's position. It is not required that you use separate certificates.

Assuming you have obtained a digital certificate from a certificate authority and have followed their directions to install the certificate, the following instructions can be used. (Installing a certificate is a fairly automated process; it will usually involve going to a link provided in an e-mail. Use Microsoft Internet Explorer to install a certificate that can be used with Microsoft Outlook; use Microsoft Internet Explorer or Mozilla Firefox to install a certificate that can be used with Mozilla Thunderbird.)

Thunderbird

If you have installed the certificate using a browser, we will first need to

export the certificate and then import it into Thunderbird. If you have the p12 or pfx file, skip to section C below.

- A.) If the certificate was installed in Microsoft Internet Explorer:
1. From the top menu select 'Tools' → 'Internet Options'
 2. Click on the 'Content' tab
 3. Under 'Certificates,' click on 'Certificates'
 4. Select the certificate and click on 'Export'
 5. Click 'Next' in the 'Certificate Export Wizard'
 6. Select 'Yes, export the private key' and click 'Next'
 7. Select 'Personal Information Exchange – PKCS #12 (.PFX)' as the format (it may already be selected)
 8. Leave 'Enable strong protection' checked and click 'Next'
 9. Enter a password twice, this password is to encrypt the certificate file, you will use this password once when importing the certificate into Thunderbird
 10. Click 'Next'
 11. Enter a file name for the certificate file (click browse to determine what folder the file will be saved in) and click 'Next'
 12. Click 'Finish'
 13. If you are prompted to allow an application to access a protected item, click 'OK'
 14. Click 'Close' for 'Certificates'
 15. Click 'OK' for 'Internet Options'
- B.) If the certificate was installed in Mozilla Firefox:
1. From the top menu 'Tools' → 'Options' (on some platforms: 'Edit' → 'Preferences')
 2. Click on 'Advanced'
 3. Click on the 'Encryption' tab
 4. Under 'Certificates,' click on 'View Certificates'
 5. Select the certificate and click on 'Backup'
 6. Enter a file name for the certificate file (click on the drop down next to 'Save in:' to determine what folder the file will be saved in) and click 'Save'
 7. Enter a password twice, this password is to encrypt the certificate file, you will use this password once when importing the certificate into Thunderbird
 8. Click 'OK' in the success

alert and 'OK' for 'Certificate Manager'

9. Click 'OK' for 'Options'

- C. Now we can import the certificate and configure Thunderbird. In Mozilla Thunderbird:
1. From the top menu select 'Tools' → 'Account Settings' (on some platforms: 'Edit' → 'Account Settings')
 2. Select 'Security' for your account
 3. Under 'Certificates' click 'View Certificates'
 4. In the 'Certificates Manager' window click on 'Import'
 5. Select the certificate that you exported above and click 'Open'
 6. If you do not already have a Master Password set, you will be prompted to set one now. This password is not the same as the password used to encrypt the certificate file, this password is used to encrypt the certificate once it is imported into Thunderbird, it is also used to encrypt any password you have saved in Thunderbird (e.g., to log into your e-mail account). Enter a password twice and click 'OK' – you will use this password often, so remember it.
 7. You will be prompted to enter the password that was used to encrypt the certificate file (IE certificate export step 8; Firefox certificate export step 7), enter the password and click 'OK'
 8. Click 'OK' in the success alert and 'OK' for 'Certificate Manager'
 9. In 'Account Settings' under 'Digital Signing,' click 'Select'
 10. Select the certificate you wish to use
 11. Click 'OK' for 'Select Certificate'
 12. You will be prompted to select the same certificate for encryption, click 'OK'
 13. Click 'OK' for Account Settings'
- To sign a new message, when in the compose message window, click the arrow next to the "Security" button with a picture of lock and select "Digitally Sign This Message;" to encrypt, select "Encrypt This Message."
- Outlook (2003 and 2007)**
1. From the top menu select 'Tools' → 'Options'
 2. Click on the 'Security' tab

3. Under 'Encrypted e-mail' click on 'Settings'
4. Under 'Security Setting Preferences' enter a name for 'Security Settings Name' (e.g. "e-mail-id smime")
5. The 'Cryptography Format' setting should be S/MIME
6. Under 'Certificates and Algorithms' click 'Choose' next to 'Signing Certificate:'
7. Select the certificate you wish to use
8. Click 'OK' for 'Select Certificate'
9. For the 'Hash Algorithm' setting, leave it on SHA1, do not use MD5
10. Click 'Choose' next to 'Encryption Certificate:'
11. Select the certificate you wish to use (this can be the same certificate used for signing)
12. Click 'OK' for 'Select Certificate'
13. For the 'Encryption Algorithm' setting, leave it on 3DES, do not use RC2 or DES
14. Leave 'Send these certificates with signed messages' checked, this will automatically provide your recipients your public key, so that they can send you encrypted messages
- 15.) Click 'OK' for 'Change Security Settings'
16. Click 'OK' for 'Options'

To sign a new message, when in the compose message window, click the button with a picture of an envelope and a gold seal with red ribbon, this is the "Digitally Sign" button. To encrypt a new message click the button with a picture of an envelope and a blue lock, this is the "Encrypt Message" button.

Exchanging Certificates / Public Keys

To allow others to send you encrypted messages, first send them a signed message. They will then be able to import your public key from within their e-mail client (Outlook and Thunderbird will do this automatically; the user will not need to perform any action). To send encrypted messages, have intended recipients send you their public key or certificate in the same way.

OpenPGP

PGP (Pretty Good Privacy) was originally developed by Phil Zimmermann (<http://www.philzimmermann.com>) in 1991. Modern PGP implementations utilize the OpenPGP standard. GPG (GNU Privacy Guard), also

known as GnuPG (<http://www.gnupg.org>), is a modern free and open source implementation of OpenPGP. Gpg4win (<http://www.gpg4win.org>) provides GPG and related utilities for easy installation on Microsoft Windows.

PGP Corporation (<http://www.pgp.com>) offers a commercial implementation amongst other cryptography products.

Thunderbird

Enigmail (<http://enigmail.mozdev.org>) is an add-on that provides OpenPGP features for Mozilla Thunderbird, it uses GPG. Enigmail is available on the official Mozilla add-on site (<https://addons.mozilla.org/en-US/thunderbird/addon/71>).

There is excellent documentation (<http://enigmail.mozdev.org/documentation/>), covering installation, configuration, and use. The short "Quickstart Guide" (<http://enigmail.mozdev.org/documentation/quickstart.php>) will get you well on your way. Consider just sending your correspondents your public key via e-mail rather than posting it to the keyserver, to avoid unnecessarily publishing your e-mail address and potential SPAM.

Outlook

Gpg4win (<http://www.gpg4win.org>) includes GpgOL, a plug-in for Microsoft Outlook to use GPG. GPG and GpgOL are all you need to use OpenPGP in Outlook; however, unlike the other options discussed above, GpgOL is still a bit too quirky to meet the stability and reliability needs of your firm.

SafeLogic (<http://www.safelogic.com>) offers cGeep (<http://www.cgeep.com/outlook-email-encryption.html>), an add-on for Microsoft Outlook that is easy to setup and use.

Popular Webmail: Gmail, Yahoo, Hotmail...

If you use a free Web mail provider for your e-mail (if you prefer Web mail, consider Yahoo or Google's paid options that allows you to use your own domain and removes ads), client-side encryption can still be easily used with a browser add-on. FireGPG (<http://getfirepgp.org>) adds a contextual menu to Mozilla Firefox that allows for using GPG features from within the browser. It is specifically designed to work with Gmail's Web mail interface (other popular Web mail providers' interfaces may also be supported in the future). If you use Microsoft's Windows Live Hotmail, the free Windows live client (<http://get.live.com>) supports S/MIME.

Alternative Webmail

Hushmail (<http://www.hushmail.com>) has both free and premium e-mail accounts. Their Web mail interface includes built in server-side encryption of e-mail (using OpenPGP) that automatically encrypts e-mails sent to other Hushmail users (or users who have uploaded their public key to Hushmail's keyserver) and offers the option to encrypt e-mails using a password to other recipients.

If your organization hosts its own Web mail system, or is considering doing so, the Horde Project's ([\[www.horde.org\]\(http://www.horde.org\)\) IMP Webmail Client \(<http://www.horde.org/imp/>\) \(also part of the Horde Groupware Webmail Edition <http://www.horde.org/Webmail/>\) includes support for both OpenPGP \(using GPG\) and S/MIME. All Horde applications are free and open source.](http://</p></div><div data-bbox=)

Be aware that while Web mail providers (including Hushmail) that provide encryption may offer a great deal of convenience over using encryption tools on your own computer (such as those discussed above), the content of the message is not kept confidential from the e-mail hosting provider.²

Encryption is an important tool for any attorney or technologist. We recommend you consider some of the tools mentioned above for the use in your home or office.

Benjamin Gerber, CISSP, CISA, CPP, CIPP/G, is a Senior Managing Consultant and Architect with IBM Security and Privacy Practice. Adam C. Nelson, Esq., CIPP, is a member of the Technology Committee of the Illinois State Bar Association and is on the Board of Editors of the Privacy & Data Security Law Journal. He is a Senior Managing Consultant in the Security and Privacy Practice at IBM. The authors can be reached at bsgerber@us.ibm.com and anelson@us.ibm.com, respectively.

1. These homeowners apparently did not sufficiently try to protect their private road enough for Google to respect the label of "private." <<http://www.informationweek.com/news/internet/google/showArticle.jhtml?articleID=208401206>>.

2. For a recent case involving this issue, see *U.S. v. Tyler Stumbo*.

Bill4Time Internet-based time and billing software

By Alan R. Press

I USED TO LOVE LOOKING AT THE BOX. In the past, when purchasing new software, I used to read the information displayed on the box and used it as my orientation to its new features and exciting capabilities. Loading new software was like taking on a brand new project. With all those welcome screens, instructions, and choices to make, the possibility of getting it all working properly was excit-

ing.

With high-speed Internet, many software vendors began allowing you to purchase software immediately on the Web and download it on the spot. No CD, no disk, and no box. However, once the download was complete, the loading of the software was pretty much the same. You just didn't have a box or a back-up disk of your purchase.

Now we have Web-based applica-

tions. No box, no disk, no CD and now, no software! You just have to subscribe (pay), get a user ID, password, and off you go. I have been using one of these Web-based applications, Bill4Time (www.Bill4Time.com) for the last few months. I have never been able to find the perfect Time and Billing Software for my solo practice. The programs are usually too complicated and cumbersome or too basic and lacking in functional-

ity. Luckily, Bill4Time has been a great solution and middle ground.

As a Web-based software program, nothing needs to be loaded on your computer. All you need is access to the Internet and either Internet Explorer, Safari or Mozilla's Firefox. This means that you may use any platform (Windows or Mac) and switch depending which computer is available to you. You may log on from anywhere with an Internet connection. Access is also available for mobile devices, including Blackberry, Palm and Windows Mobile. If you use Microsoft Windows and Quickbooks, there is a link that allows you to integrate Bill4Time with your billing and receivables in Quickbooks. I tested the link and it was easy to install and use.

Set up was simple and straightforward. I was quickly adding clients,

recording time and generating invoices. With all of this simplicity come some limitations in flexibility and customization, but that criticism is far outweighed by the tremendous usability and intuitive interface and menus. A "dashboard" link is always available and quickly gives you a listing of active clients and all the popular task buttons. Navigation through the program is very simple. The bills look professional and some customization is possible. Multi-users and timekeepers are fully supported.

Bill4Time gives you a free 30-day trial without having to give your credit card information. I ran it for a month concurrent with Timeslips and decided to keep Bill4Time. I am much more comfortable with the ease of use and the ability to use Bill4Time on any platform (as I have a Mac notebook).

I also love the way that Web-based applications do not eat any of your system's resources. I leave myself logged-in all day (I have the program open on its own tab in Safari and you could do the same with Explorer or Firefox), and I find it a cinch to record my time. I never have to worry about back-ups for the data, although I am able to export data at any time to an excel spreadsheet. In addition Bill4Time is continually updating and improving the program. There have been updates each month and you never have to load anything. It is all there by virtue of logging in!

Customer support is very accessible and responsive. It seems like a small company, one that is very hands-on. Bill4Time may not be perfect for everyone, but why not give it a look?

ISBA's 4th Annual

Solo & Small Firm Conference

EXPANDING Your Network Knowledge and Skills

September 4-6, 2008 • Pheasant Run Resort, St. Charles, IL

Illinois' premiere event for solo and small firm lawyers.

Gather with your colleagues for a weekend of insightful programming and networking opportunities at the ISBA's Solo & Small Firm Conference. Choose from three program tracks - *Substantive Law*, the *Effective and Ethical Practice of Law* and *Legal Technology* - to earn up to 14 hours of MCLE, including all 4 hours of professional responsibility MCLE.

Featured Speakers



ELLEN FREEDMAN, CLM

Law Practice Management Coordinator
Pennsylvania Bar Association
Founding Partner – Managing Partner
Development Institute™



ROSS L. KODNER

President/Founder
MicroLaw, Inc.
Technology Consultant



NERINO J. PETRO, JR.

Law Practice Management Advisor
State Bar of Wisconsin

One plenary program.
Three tracks.
Forty sessions.

Numerous learning
opportunities.

**TO FIND OUT MORE
OR TO REGISTER**

www.isba.org/solo2008

(800) 252-8908

infoSSFC@isba.org



Do yourself a favor

Say goodbye to paper and get this newsletter electronically

Why?

You'll get it faster. Opt for the electronic version and bypass the ISBA print shop and post office. We'll send you an e-mail message with a link to the latest issue as soon as it's posted on the Web, which means you'll get it days, even weeks, earlier than you would in print.

You'll save space. Because newsletters are archived on the ISBA Web site, you needn't worry about storing back issues.

You'll help keep section fees low. At \$20/year, section membership is a tremendous value. But paper and postage costs continue to rise. By choosing the electronic over the paper version, you help keep our costs—and yours—down.

How?

Just go to <<http://www.isba.org/newsletters/enewsletters.html>>. Submit an easy-to-complete form and have any newsletter—such as the next issue of *Legal Technology*—delivered to your inbox.



Non-Profit Org.
U.S. POSTAGE
PAID
Springfield, Ill.
Permit No. 820

Legal Technology
Illinois Bar Center
Springfield, Illinois 62701-1779
August 2008
Vol. 16 No. 2