CPCU SOCIETY INSURING YOUR SUCCESS

Information Technology Interest Group

Cutting Edge

Volume 16 • Number 2 • August 2009

Make Your Interest Group Selection Now to Be Included on the New Mailing List

To continue receiving a printed newsletter or to opt for electronic notification of the latest issue, you *must* choose a primary area of interest — if you have not yet done so. Go to www.cpcusociety.org, log in and click on "Interest Groups." For assistance, call the Member Resource Center at (800) 932-CPCU, option 4. Of course, as a paid Society member, you have electronic access to all interest group newsletters.

A Word from the Editor

by Celeste Allen, CPCU, CLU, ChFC, FLMI

Celeste Allen, CPCU, CLU, ChFC, FLMI, has 28 years' experience in the insurance industry, having worked in claims, underwriting, business analysis and information technology. She currently is a manager with State Farm. Allen's leadership experiences led her to strengthen her community service participation and make a difference in the lives of young people in her community, including those at-risk. Allen also is a member of two major public service organizations. She earned a bachelor's degree in psychology from Temple University, a master's of business administration degree from Illinois State University and a master's degree in executive leadership from the University of Nebraska at Lincoln.

The end of summer usually represents a time to get ready to go back to school. But it can also be a time for you to "virtually" take the opportunity to advance your technical knowledge, acumen and skills.

We are surrounded by technology and perhaps take it for granted. From business and personal perspectives, the use of technology has vast implications. In this issue, we examine the use of personal computing on another level:

- How insurers can gain a competitive advantage by desktop virtualization.
- How our social interactions can be leveraged for business and personal use.
- How we need to be attuned to the legal implications of Web 2.0.
- How insurance can offer protection against cyber crime.
- How the auto black box may aid crash investigations.

Take a moment to assess the technology you use on a daily basis in the workplace and for personal use. You do not operate in a vacuum — you are connected by and to a vast array of networks.

Turn a new leaf on your business life and take the time to learn, grow and increase your value to your organization. ■

What's in This Issue

Looking for Ways to Be More Competitive? The Solution Could Be Right on Your Desktop

Desktop Virtualization Saves Money, Reduces Risk and Improves Business Agility

by Thomas J. Filep, CPCU

Thomas J. Filep, CPCU, is a partner and an insurance industry expert in Computer Science Corporation's (CSC) financial services practice. CSC is a leading global consulting, systems integration and outsourcing company. Filep is a past president of the CPCU Society's New Jersey Chapter, and currently serves on the chapter's board of directors. He is also a member of the Information Technology Interest Group. He can be reached at tfilep@csc.com or by phone at (908) 392-6511.

The insurance sector is gradually regrouping from unprecedented economic instability, unfavorable investment returns and increased combined ratios; and carriers are looking for new ways to gain the competitive edge in this uncertain market.

Believe it or not, the solution could be sitting right in front of you — instead of your PC. That's right, your desktop PC is one of the things holding your organization back. Consider the cost of buying and repairing PCs, the downtime associated with maintaining them and the relatively lax security that could expose sensitive customer information to theft and fraud.

That's why a growing number of companies, including Computer Science Corporation (CSC), are moving to desktop virtualization. By replacing PCs with thin-client devices, organizations are using desktop virtualization to lower costs, improve compliance and security, and gain agility to meet customer expectations.

What is desktop virtualization and how does it help insurance companies improve their competitive positions?

Desktop virtualization is the process of separating personal computer desktop applications, data and files from the physical machine. The applications and the user's view of the desktop are then delivered from a central data center, which is a natural extension of the managed desktop model. As a result, end users are able to remotely access their desktops and work product on any device that is able to display the desktop. The device might be a desktop PC at a telecommuting home office; desktop on a thin client in the home or satellite office, the hotel or airport; or desktop applications on a smart phone.

Desktop virtualization offers significant advantages in the areas of cost reduction, risk management and business agility:

(1) Cost Reduction.

- Longer asset life — Lower desktop computing resource requirements result in an extension of the useful life of assets from as short as three to more than seven years.
- Lower annual access device cost — Annual cost per device can be reduced by as much as 50 percent over the useful life of a conventional business PC versus a high-end thin client as a result of longer times between refresh cycles.
- Reduced power usage — Power savings of greater than 80 percent are possible when switching from a conventional mid-range PC to a high-end thin client. Also, energy savings for multiple applications and low utilization on one piece of hardware.
- Utility pricing — Predictable ongoing costs that scale with employee growth. Monthly per user costs can be reduced by more than 25 percent versus a traditional desktop.
- Software license management — Software license management is built into this centrally managed service, which allows for almost immediate audits of existing software installations in the company with no added cost.

(2) Risk Compliance and Security.

- Secure data access — Every login session is established via the virtual desktop infrastructure.

- Automated backup — Data resides on home and profile directories rather than locally, eliminating individual device backups and data recovery costs.
- Data risk — All computers and their associated data are centrally controlled, which enhances compliance and improves data security. This reduces loss of data that might occur through theft of laptops, accidents or employee turnover.
- Reduced potential infection rate and reduced remediation time — Because a single consistent desktop environment is maintained across the entire user base, virus protection and remediation efforts can be deployed in real time to all users.
- Disaster recovery and business continuity planning dramatically simplified for field office locations — Should a disaster interrupt operations at a field office, users can access their desktop environments through a variety of alternate methods.

(3) Improved Business Agility.

- Mergers, acquisitions and expansion — Organizations can add new users rapidly, which allows stakeholders to react much more quickly to M&A and expansion opportunities.
- Rapid deployment/upgrades — New users and upgrades can be deployed in minutes, assuring all users have up-to-date applications and security features.
- Vendor integration — Business partners and vendors can be given access based on their user type, shortening the time needed to provision nonemployee users.

- Anytime, anywhere access — Authorized employees, contractors and services providers will be able to securely access their desktop from almost anyplace with an Internet connection and suitable access device, including PDAs and smart phones.
- Improved end-user experience — End users have a fully customized experience available from any compliant computing device. In addition, their desktop sessions remain active and unchanged even when moving from device to device.
- Limited downtime for end users when hardware failures occur — When failures occur, replacing an access device takes minutes rather than days.

Here are practical business examples for desktop virtualization:

- Global insurance company — Implement for employees with international travel commitments and unique need to maintain data in home country due to high security context. With desktop virtualization, display devices are secured through an encrypted USB stick, which controls access to each employee's desktop environment. Multiple applications are delivered through a combination of application streaming and traditional methods.
- Domestic/regional insurer — Host virtual desktops to accommodate field and virtual employees with a thin-client solution, which will minimize endpoint computing requirements, stream virtualized applications and provide flexible packaged services to optimize business results.
- Insurer with multiple datacenters — Virtualization services are useful for insurers with multiple call or datacenters and global deployment needs. A virtual desktop environment based in Europe can also serve North American users. Data analysis and migration are performed to find the best-suited solution, including a mix of traditional and streamed applications when warranted.

Each insurance company business model has the potential to achieve breakthrough savings and improvements to operations. So, the next time you're looking for ways to become more competitive, look no further than your desktop. Desktop virtualization is a prudent consideration to reduce cost, improve compliance, and uphold security and business agility. ■

Legal Implications of Web 2.0 and Social Networking in Business

by Roy E. Howton Jr., CPCU, ARM, AAM

Roy E. Howton Jr., CPCU, ARM, AAM, is currently a senior software engineer for Crawford & Company, based in Atlanta, Ga. He began working for Crawford & Company in 1976 as a claims adjuster. In 1989, Howton's career changed directions as he began working in Crawford's Risk Sciences Group (RSG), helping to create and maintain risk management information systems for RSG's clients. He has two undergraduate degrees from Rensselaer Polytechnic Institute, in Troy, N.Y., and is currently a graduate student in information systems at Kennesaw State University, in Kennesaw, Ga. Howton, an Atlanta Chapter member, obtained his CPCU designation in 1985. He also has earned the Associate in Risk Management (ARM) and Associate in Automation Management (AAM) designations.

Web 2.0, as it has been called, is a new way of working on the Internet. Powerful new tools allow individuals and businesses to create dynamic Web pages for communications, knowledge transfer and socializing. These new tools are quick and easy to use and can be utilized by employees with very little training. While Web sites are still used for displaying and retrieving information, with many of the new Web 2.0 Web sites, however, users can add, edit and respond to the information found on these Web sites. On social networking sites, users create their own Web pages to display both personal and professional information. Businesses use these Web sites to reach more potential customers faster than other methods of the past.

Along with the new capabilities come some risks. The new Web sites make it easy for anyone with access to post material and make statements that may put the individual or business at risk. Individuals as well as businesses must be aware that laws and etiquette still apply to these Web sites. Policies need to be established to see that laws are not broken.

What Is Web 2.0?

More and more companies are exploring the landscape of social networking for business communication practices. One of the main components of social networking is a technological phenomenon known as Web 2.0. There does not seem to be any one definition for the term, Web 2.0.

Web 2.0 would seem to refer to a new version of the Web; however, there is no new Web, just new ways to utilize the Web. These Web 2.0 applications run entirely through an Internet browser and are not tied to the user's personal computer. The Web has evolved from being a look-up and retrieve-only tool to one that allows users to interact and collaborate.

What Comprises Web 2.0?

A range of new applications have contributed new words to the English language, such as blogs, wikis, mashups and folksonomies. A wiki is a Web page that allows anyone with access to the page to make changes to the page. Blogs are typically used by individuals to provide online commentary on a subject that holds a particular interest for the writer and the reader. A mashup is a result of combining data or features from one or more unrelated Web sources to create a new unanticipated use for the data or features in a new application. A folksonomy is a collection of tags or bookmarks that have been used by individuals to indicate their preference for an item or idea. As a result of the interactive nature of these applications, new social networking Web sites have sprung up all over the Internet. These social networking sites allow individuals to create profiles featuring things about themselves that they want to share among a group of friends or the world.

The most popular sites include FaceBook, MySpace, Twitter and LinkedIn. These sites allow users to share personal and sometimes sensitive information with anyone who has access to their profile. Both FaceBook and MySpace started out as a way for individuals to share personal information among friends. Now, companies like Forrester, Proctor & Gamble, Ernst & Young and IBM are encouraging their employees to create Facebook profiles. (Kirkpatrick, 2008)

LinkedIn is more business-oriented and is almost like a contact application that is centered on business résumés and where one can keep track of business associates. Twitter allows users to send other users blog updates, or "tweets," up to 140 characters as a way of keeping each other abreast of their current activities.

Why Do Businesses Want to Use These Applications?

Companies are using Web 2.0 technology and applications because the tools are easy to implement. Many companies report that implementation of these tools began at the grassroots level of the organization. Small groups are then used to test the results. (*The McKinsey Quarterly*, 2007)

Companies are using blogging systems rather than e-mail to combine Web-based blogging and content management to reach wider audiences. In this manner, the organization is neither limiting its audience nor having to predetermine what its audience might be. This enables the organization to solicit and obtain ideas and opinions from individuals at all hierarchical levels of the company. In other companies, blogs are being used to directly talk to customers and other company stakeholders.

What Legal Implications Arise from Using These Applications?

As a result of the information on a Web 2.0 Web site coming from multiple and sometimes uncontrollable sources, new legal issues can arise in addition to the ones normally encountered by an

organization. These organizations must be aware that online activities are subject to the laws of various jurisdictions. Issues arise concerning copyright laws, trademark, invasion of privacy, defamation and trade secrets.

Copyright Laws

Copyright laws vary throughout the world; however, most serve to grant specific rights to the creator of an original work. These rights are generally protected for a specific length of time. The rights granted by copyright laws to the creator of a work include the right to copy or reproduce the work, to perform or display the work, and the right to sell or assign these rights to others.

Companies transmitting or generating consumer-created data must determine who owns the copyright. Businesses can receive some protection from copyright laws depending on their relationship to the creator of the work. Section 201(b) of the Copyright Act declares that in the case of a work-made-for-hire, such as work performed by an employee, the employer is recognized as the owner of the work and thus entitled to all copyright privileges unless there is an agreement between the employee and the employer to the contrary. When the work, however, is performed by an independent contractor, as defined by common law, the U.S. Supreme Court in *Community for Creative Non-Violence v. Reid* essentially found that contractors work will not fall under the case of work-made-for-hire.

Of course, there is always an exception, and in this case if a contractor's work falls under Section 101(1) of the Copyright Act and the work is commissioned for a collective work (as in the case of a motion picture, a translation, a supplementary work, a compilation, an atlas, an instructional text, a test, or answer material for a test), then when the parties agree in writing, the work qualifies as a work-made-for-hire. When a work is performed by an independent contractor, even in the case where there is an agreement stating that the rights of copyright are assigned, the copyright remains with the contractor. In this case, a contract must be written to have the contractor assign all rights to the work to the employer. (Burgunder, 2007)

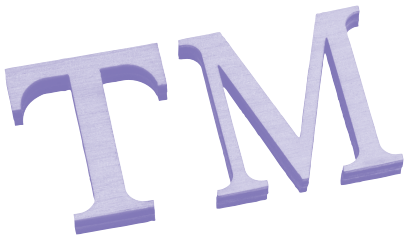
With the implementation of the Internet, and now with Web 2.0 applications, it is easy for many individuals to get the impression that all material found on the Internet is free for the taking. Some of this is due to ignorance; however, the taking of material that belongs to someone else and claiming it as original is illegal. Copyrights are still valid legal rights held by the creators of the material and cannot be ignored. Many social networking users add music, photographs, videos, and other literary contents that are protected by copyright to their user profiles. Businesses requesting that their employees create profiles or produce wikis that can add this type of data would be wise to develop policies against the use of this material or, if it is used, to make sure that it is done with the permission of the copyright holder.

Issues with Web 2.0 collaborations have to do with determining the owner of the material placed on these sites, and, if there are international contributors, determining how to deal with the different jurisdictional requirements. There are also questions that will arise with regard to the use of exceptions, such as fair use and its jurisdictional requirements. (Web2Rights, 2008) In the U.S., one of the main limitations to copyright is the doctrine of "fair use." This doctrine came about through a series of court cases over the years and was finally codified into the Copyright Act as Section 107. There are certain situations where reproduction of copyrighted work may be considered fair. These situations include when a work is being criticized; a commentary; when it is newsworthy; and for teaching purposes, scholarship and research. (U.S. Copyright Office, 2006)

Four factors are to be considered for determining fair use:

- The purpose of the use and whether it is for profit or nonprofit.
- The nature of the copyrighted work itself.
- The amount of the copyrighted material actually copied.
- The economic impact the use may have on the value of the copyrighted work.

There are times when a fine line exists between fair use and infringement. Businesses and individuals would be wise to seek the advice of counsel if there is any question about whether using copyrighted material meets the qualifications of fair use (U.S. Copyright Office, 2006)



Trademark

The Lanham Act created the U.S. Federal Trademark statute. The purpose of the statute is "to protect words, names, symbols, or devices that serve to distinguish the sources of goods or services." (Burgunder, 2007) Trademark owners can be registered or nonregistered. Registered trademarks are typically enforceable throughout the jurisdiction granting the trademark, whereas nonregistered trademarks may be limited to specific geographical areas where the trademark is known. Trademark owners are responsible for initiating the legal

Continued on page 6

Legal Implications of Web 2.0 and Social Networking in Business

Continued from page 5

procedures necessary to induce infringers to cease and desist using their trademark.

According to a blog on SEOmoz.org written by attorney Sarah Bird (Bird, 2008), the shoe retailer DSW filed suit in 2008 against Zappos.com and Commission Junction for trademark infringement. DSW operated a Web site (DSWshoes.com) since 2000 to promote its physical stores but not to sell shoes online. In 2008 DSW began to sell shoes directly through DSW.com, its new online store.

Zappos is an online shoe retailer that maintains an affiliate campaign with Commission Junction. Some of the Zappos affiliates created Web sites such as dswreview.com and dsw-shoes.net. The review sites were allegedly favorable to DSW and included DSW photographs. The sites included a link to the Zappos site, but not to DSW.

Shortly after DSW opened DSW.com, it filed suit against Zappos for trademark violations stemming from the Zappos affiliates use of DSW trademarks. Questions arise as to the relationship that Zappos has to its affiliates. Are the affiliates agents of Zappos? Does Zappos have control over the actions of its affiliates? Here it would appear we have a trademark action that is also dependent on the common law agency relationship.

Based on this, it would appear that the Zappos affiliates' use of the DSW name and its photographs would be an infringement of the DSW trademark. One of the main questions is: Would the average consumer be confused by the site and would they expect links to take them to the DSW site? The courts will ultimately decide, but this case shows how Web 2.0 technologies can get companies who are not diligent about determining whether a trademark exists in legal trouble.

Defamation

Defamation occurs when one publicly makes a false statement about someone else and that person's reputation is harmed as a result. There is an exception to this as the result of a ruling on the case *New York Times v. Sullivan*. In this case, the U.S. Supreme Court held that "the First Amendment protects the publication of all statements, even false ones, about the conduct of public officials except when statements are made with actual malice ... ." (Oyez Project)

The Communications Decency Act, created as part of the Telecommunications Act of 1996, creates a safe harbor for online service providers that shields them from liability for their users' actions and related content. As a result of this legislation, courts have interpreted Section 230 of this law as providing online service providers and Web site operators with immunity from primary and secondary liability for claims, including "defamation, employment torts, negligent misrepresentation, cyber-stalking, and breach of contract." (Ziniti, 2008)

As a result of the information on a Web 2.0 Web site coming from multiple and sometimes uncontrollable sources, new legal issues can arise in addition to the ones normally encountered by an organization.

Prior to the Internet age, it was relatively difficult to broadcast a defamatory statement unless you were a reporter, a writer or a famous orator. In the case of the printed word, editors are in place to control what is printed. With companies utilizing wikis, blogs and other social networking tools, it is now easy for a defamatory statement to make its way around the world in relatively little time. (Burgunder, 2007)

Invasion of Privacy

Many businesses are now using social networking sites to obtain information about current employees and job applicants when making personnel decisions. In many situations, when an individual creates a social networking file and then makes it public, it is hard for that same individual to cry foul when an employer accesses this public site and gains negative information. However, if the employer, for the purpose of personnel decisions, creates a user to become "friends" with an employee who has made his information only available to friends, then that employer may be guilty of invading the privacy of the employee. (Brand & Scherwin, 2009)

Over the past few years, new technological devices, such as mobile telephones with photography and videography capabilities, have allowed individuals to be photographed without their knowledge or in situations that they would have considered private. These photographs, coupled with social networking sites, can now be made available to the world. As recently as a few months ago, a photograph of Olympic medal-winning swimmer Michael Phelps taking a hit from a bong made news when that photograph became public. In this particular case, the photograph was released through an old-fashioned newspaper, but once available there, the news and the photograph traveled rapidly and far via the Internet.

I am sure that Phelps either never knew that the photograph was being taken or never expected that it would become public. Phelps is not only a swimmer, but a business. In his particular case, Phelps, being a so-called public figure, is probably used to very little private life. As a result of this photograph, however, he lost sponsorships, was suspended by USA Swimming for several months, and suffered a diminished reputation. In addition, this photograph led to a police investigation for possible criminal activity.

Dan Findlay, in the *North Carolina Journal of Law and Technology* (February 2009), explores issues such as those faced by Michael Phelps. Essentially, it is the age-old question of whether the law is keeping

up with technology. It is his opinion that the government's accessing and using photographs taken with or without an individual's knowledge may constitute an invasion of privacy. Certainly, times have changed with regard to what may be considered private, as well as what is public information. Careers and businesses can be ruined by an untimely photograph or a wrongly interpreted statement. In the past people needed to be wary of what was said to a reporter or they could find their statements in print or the subject of a TV news story. Today, people need to be wary about what they say to friends or colleagues, as they have as much circulation capabilities with blogs and social networking as does a reporter.

Discrimination

Some jurisdictions, such as California, have rules regarding the information that employers can use to make employment decisions. Typically, categories such as sex, race, disability and age cannot be used in making personnel decisions. An employer that uses a social networking site and discovers that the employee or prospective employee has a disability and then denies employment based on this knowledge may be subject to a discrimination suit. (Brand & Scherwin, 2009)

Trade Secrets

The Uniform Trade Secrets Act (UTSA) defines a trade secret as information that has economic value because it is not known or easily attained by others who may benefit, and reasonable steps have been taken to maintain its secrecy. Web 2.0 technologies offer another avenue for a company's secrets to escape the confines of its secrecy protection. Once a secret becomes public, the protection afforded under the UTSA is no longer useful.

How Can Businesses Lessen Their Exposures to Liability from Using Web 2.0 Applications?

Some businesses have banned the use of social networking sites due to the potential risks faced. However, to do so keeps the company from reaping the benefits that might accrue from the use of these sites. Companies that decide to allow the use of these sites need to develop policies to govern employee access and stipulate the locations to which access is allowed.

Employees should be cautioned about the information that they post in wikis, blogs, and the like, as well as coached in what types of information can and cannot be posted. Policies concerning trade secrets should already be in force, but employees should be cautioned again about the importance of this information and the need to keep it secret. All parties not employed by the company, but with access to company intranet services, need to have formal approval to access these sites. Nondisclosure agreements need to be obtained for anyone that has access to company secrets. (Stephens, 2001)

The Digital Millennium Copyright Act provides safe harbors that can protect an organization from legal liability when it uses and enforces a copyright policy. This policy must also provide a means by which those who see a copyright violation can report the offense and have the material removed. This can be helpful in offering some protection to user-generated content sites such as blogs, wikis and social networking sites.

With regard to copyrighted material, tools exist which allow the Internet to be searched to determine if a work has been plagiarized. Any material that is used in company Web sites, blogs, or wikis that is not produced in-house needs to be perused for possible copyright infringement, and any offending material removed.

Conclusions

Technology seems to always offer new and exciting tools to enhance how we live our lives and conduct business. As always, what seems to lag behind is our ability to cope with these new tools, given our excitement over using them. Just because you can blog doesn't mean you should. Unfortunately, there is a tendency to see what the competition is doing, and then the race is on to compete. As with all things, there are risks. The prudent business will develop a plan, and then develop guidelines and procedures on how to utilize these tools. Businesses that shun these tools because the risks are too great will suffer, as the potential to the business for marketing, developing new products and communicating, both internally and externally, is just too great.

As always, the goal should be balance. Companies that place too many rules on the use of wikis, blogs or other tools run the risk of negating their usefulness. One of the greatest features of these applications is the freedom of expression allowed by them. Too many rules on their use will just deter people from contributing to them any longer. The fact that IBM can get 150,000 stakeholders together and from that get 46,000 ideas for different business opportunities is mind boggling. The legal landscape is the last to respond to new innovations. This is to be expected, as laws should only be passed when the rules that exist can no longer fairly control the matters at hand.

Most intellectual property laws seem to be well-positioned to handle the new world. A possible exception to this may be the copyright laws, as they pertain to expressions in group collaborations. The main concern, legally, is the right of privacy. The combination of cameras and other recording devices with social networking sites can quickly create a public sensation out of what was thought to be a very private moment. Unfortunately, the subjects of these newsworthy exposures have little legal

Continued on page 8

Legal Implications of Web 2.0 and Social Networking in Business

Continued from page 7

recourse. Sooner or later, what affects individuals will soon affect businesses, and then we will see the laws change.

Blogs, wikis and social networks are here, and will only become more and more embedded in mainstream global business. As with all things with great potential, there are risks. It is the business that plans and embraces these changes that will be the one that succeeds. ■

References

Baker, S. and Adomaitis, M. "Advantages of Networking in Business." LoveToKnow. 2008. Retrieved April 22, 2009, from http://socialnetworking.lovetoknow.com/Advantages_of_Networking_in_Business.

Bird, S. "DSW Sues Zappos.com for Trademark Infringement over Affiliates' Review Sites." SEOmoz. 2008. Retrieved April 21, 2009, from http://www.seomoz.org/blog/dsw-sues-zapposcom-for-trademark-infringement-over-affiliates-review-sites.

Brand, R. and Scherwin, T. "Employers That Use Social Networking Sites Face Legal Risks." *Talent Management Perspectives.* March 2009. Retrieved April 22, 2009, from http://www.talentmgt.com/newsletters/talent_management_perspectives/2009/March/889/index.php.

Burgunder, L. *Legal Aspects of Managing Technology.* Thomson Learning: 2007, 4th ed.

Business Technology Office, Media & Entertainment Practice, McKinsey & Company. "How businesses are using Web 2.0: A McKinsey Global Survey." *The McKinsey Quarterly.* March 2007. Retrieved April 19, 2009, from http://www.mckinseyquarterly.com/Marketing/Digital_Marketing/How_businesses_are_using_Web_20_A_McKinsey_Global_Survey_1913.

Dearstyne, B. W. "Blogs, Mashups & Wikis: Oh My!" *Information Management Journal:* July 2007, Vol. 41 Iss. 4, pp. 25-33.

Findlay, D. (February 2009). "Tag! Now You're Really 'It.' What Photographs on Social Networking Sites Mean for the Fourth Amendment." *North Carolina Journal of Law and Technology.* February 2009, Vol. 10 Iss. 1., p. 171. Available at http://cite.ncjolt.org/10NCJLTech171.

Kirkpatrick, D. "Web 2.0 gets down to business." CNNMoney.com. March 25, 2008. Retrieved April 19, 2009, from http://money.cnn.com/2008/03/19/technology/web2.0_goofing.fortune/.

The Oyez Project. *New York Times v. Sullivan.* Docket No. 39: Ruling 03/09/1964. Retrieved April 21, 2009, from http://www.oyez.org/cases/1960-1969/1963/1963_39

Stephens, D. O. "Managing Records and Information in Web Environments: Policies for Multinational Companies." *Information Management Journal.* April 2001, Vol. 35 Iss. 2, pp. 64-67.

U.S. Copyright Office (2006). Fair Use. Retrieved April 24, 2009, from http://www.copyright.gov/fls/fl102.html,

Web2Rights. "Web 2.0 and IP Factsheet." Higher Education Funding Council for England (HEFCE): March 28, 2008. Retrieved April 19. 2009, from http://www.web2rights.org.uk/documents.html#a1.

Ziniti, C. "The Optimal Liability System for Online Service Providers: How *Zeran v. America Online* Got It Right and Web 2.0 Proves It." *Berkeley Technology Law Journal.* Annual Review 2008: Vol. 23 Iss. 1, pp. 583-616.

Technology in the Cloud

by Celeste Allen, CPCU, CLU, ChFC, FLMI

Clouds abound in the sky, and looking up to them in wonder and amazement, we can search for a hint of rain or discover a beautiful backdrop for a landscape. Clouds are all around us, physically and virtually. If you're a user of the Internet or a mobile phone, or own a smart phone or other handheld device, then you are in the "cloud."

A cloud is a "centralized network made up of hundreds of thousands of servers, each storing staggering amounts of data." It can also consist of resources and services provided over the Internet as well as provision of online computing and computing capacity from data centers. (Orange 2009)

Clouds come in three varieties (unlike Bubba's unending list of shrimp dishes in the movie *Forrest Gump*). A public cloud is open, located externally, accessible to the public, and its use is accomplished via free, rental or subscription to space and services. A private cloud is custom built, contains firewalls, has greater reliability and is available at a high cost. A hybrid cloud combines the advantages of public and private clouds and is used frequently to bolster an existing computer infrastructure.

Business Implications

Cost savings and reduction of operating expenses can be realized via mining and managing data on an enormously large scale via cloud computing. How well you get along with others on your team or how well your group communicates across departments and across functions can be assessed via cloud computing. Departments within an organization can share a single database, where previously each maintained similar data stores.

Workplace relationships may be predicted to reveal conflicts, employee satisfaction, productivity and financial risks. Information can be leveraged to possibly attain competitive advantages via assessing trends in consumer consumption of goods.

Collaboration and communication styles of an organization can be assessed as well as, for example, frequency of breaks. (Yes, you've been spending too much time at the watercooler.)

Startup companies will have the ability to access a vast amount of power without having to undertake substantial investments in hardware and software.

Avon Products is changing the way it manages six million sales representatives, from face-to-face and phone updates to equipping 150,000 sales leaders with smart phones connected via a cloud-based computing system to monitor and track sales of representatives. Serena Software primarily uses cloud services and uses Facebook for internal communications. Coca Cola provided 40,000 mobile workers with portable devices that allow them to be connected with the office while traveling. Software applications once handled in-house are now being handled by cloud systems.

Personal/Social Implications

Whether you use the Internet to bank, make a purchase online or comment on a blog, you're in the cloud and maybe didn't even know it! So, how did this happen? Well, if you use a laptop computer, mobile phone or the GPS system in your car, you opened the door and stepped into the cloud via "cloud-based end-user applications." (Orange 2009)

A large number of activities conducted on the Internet are tracked, and as business futurist Erica Orange states in *The Futurist* magazine, they "leave a trail of digital breadcrumbs." Social networking software and GPS-enabled devices provide users of services such as Brightkite with information based on location (known as geotagging) as well as with instant messaging. Social networking can be used to identify patterns in social relationships. Information gleaned from sensors is referred to as reality mining. Why even those in search of relationships can use Serendipity software to meet up with that special someone.

While a plethora of information is gathered from sites such as Facebook, Twitter and MySpace, research is underway to assess how to build in-depth profiles through the use over time of algorithms from digital data. From

Continued on page 10

Technology in the Cloud

Continued from page 9

a health perspective, speech analysis software and sensors could provide information on looming health issues. FriendFeed is software that allows bundling of all online activities broadcast to online friends via a single broadcast.

The Good, the Bad and the Ugly

Google foresees future applications maturing to the point where it will be able to advise customers on careers and leisure activities. It may be possible in the very near future for companies to offer software that can provide the best dining places for a customer. Companies such as Intel, IBM and Research in Motion are striving to apply personal-touch-based services provided by Apple and Google. This past spring, IBM launched internally collaboration and social networking software — LotusLive Engage — and will market same to its customers in the form of cloud services.

OK, there's the cliché, "Don't rain on my parade," and there's a new possible cliché, "Don't let it rain on my cloud." (Okay, okay, just work with me.) Security and the loss of control of personal data are major concerns. Personal information such as address, telephone numbers, marital status and criminal record are already available online. The government and companies (vendors and employers) can use information gleaned from location-tracking technology to provide insight into consumer and employee behavior, perhaps to the extent of predicting behavior. Once obtained, there is no expiration label on digital data, and per Orange, once personal information is stored in a cloud, it is no longer considered personal property and legislative action may be warranted to lessen privacy risks.

Reliability is a requisite for cloud services, yet glitches can happen; and when they do, they have vast impacts. For example, an outage experienced by Google on May 14, 2009, left customers without the use of its online services. How many times a day or week do you use Google services? Now imagine a day without them!

Conclusion

Cloud computing offers not only expense savings but also untold tracking and connectivity capabilities. Stay tuned for what's coming down the pike as businesses work to streamline and merge cloud services. There's no longer a need to keep your head out of the skies when your technology can take you far into the cloud. ■

References

Cohen, Aaron M. "Types of Clouds." *The Futurist,* July/August 2009, Vol. 43 Issue 4, p. 18.

Hamm, Steve. "Cloud Computing's Big Bang for Business." *BusinessWeek,* 6/15/2009, Issue 4135, pp. 42-44.

Orange, Erica. "Mining Information from the Data Clouds." *The Futurist,* July/August 2009, Vol. 43 Issue 4, pp 17-21.

'Silent' Passenger

The Auto Black Box Today and in the Future

by Peter R. Thom

Peter R. Thom is principal of Peter R. Thom & Associates Inc., a national firm of consulting automotive engineers.

Contributor Ryan Devine is a managing engineer at Peter R. Thom & Associates Inc.

Editor's note: (1) This article originally appeared in the Wednesday, Oct. 22, 2008, issue of *Claims Advisor* magazine and is reprinted with permission. (2) This article first was reprinted in the August 2009 issue of the CPCU Society's Personal Lines Interest Group newsletter.

The dawn of a new day brings another gadget onboard the automobile. Behold the Black Box, or, more accurately, the automotive event data recorder (EDR) — a nondescript piece of technology that spends most of its functional life waiting for an electronic wakeup call from a car's airbag safety system to fulfill its mission.

Its anonymous cladding, though, obscures a controversy. This little piece of technology recently has been troubling consumers, the courts, insurance carriers, lawyers and regulators. Even while it promises answers to automotive claims, it's also triggering questions about judicial admissibility, insurance coverage, privacy rights, regulatory concerns and technological capabilities. Many of the questions can be answered with a better understanding of the technology and its implications, while others will be resolved over time as the EDR technology matures.

As a frontline representative for your carrier, you're not only a consumer concerned with the personal ramifications of the technology, but you must present your company's perspective as well. Here we'll take a look from both sides.

Big Brother

Ever since George Orwell released his classic novel *1984* in which he described a totalitarian society where it was announced that "Big Brother is Watching You," people have been leery about losing control of their privacy. The big question is: Can the EDR spy on me as I drive? No. The EDR is a data-gathering module located in your car's airbag control system that is designed to collect specific data in case of deployment — no microphones, no cameras. The EDR is unlike OnStar by GM or similar products that have communications, in-vehicle security, GPS and remote diagnostics capabilities. Their satellite and real-time monitoring make them more vulnerable to questions of privacy invasion than the EDR.

When airbags don't function as designed, automakers become liable for the injuries sustained by drivers and passengers. The EDR was developed to collect operational information about airbags so performance could be improved. It was a very short jump then to apply the technology to the needs of regulatory agencies, like the National Highway Transportation Safety Administration (NHTSA), which require real-world crash statistics for highway safety research. Then, add accident investigators, attorneys and insurance carriers who want access to accident data for their own purposes, and suddenly the EDR becomes a child caught in a custody battle among groups with conflicting needs and interests.

The result is that the EDR is now being re-engineered by the NHTSA and other interested parties to meet operational and reporting standards for a broader audience — although these parameters will apply only to automakers who install EDR modules in their airbag systems, with voluntary compliance set for 2010. To be clear, not all cars have EDR modules in their airbag control systems — the NHTSA estimates 64 percent of model year 2005 have some EDR capability. Those numbers certainly will increase over time, but at this point it is an automaker's decision whether or not to install EDR.

What Is the EDR?

The EDR is a box of circuitry attached to the airbag module that will collect operational information if the airbag deploys. An important detail: There are crashes and near crashes in airbag lingo. The airbag deployment module activates when it suspects an accident is in the offing, and that is known as a "near crash." The system is ready to react, but the airbag does not deploy. The EDR will store near-crash data until it's overwritten by another near-crash or crash event. It's the crash event that is significant here — that's the data accident investigators will harvest.

What turns on the airbag deployment system? Sudden changes in speed. When rapid accelerations or decelerations occur, the EDR system wakes up and does two things. First, the EDR takes the data it has been sampling every second and saves the last five seconds of it. This data includes vehicle speed and engine RPM, and also may include seatbelt buckling, brake application, shifter position, cruise control settings and throttle setting. Secondly, the EDR records the subsequent rapid changes in vehicle speed which describe the behavior of the vehicle during the collision. This second type of data sampling may occur for a fixed amount of time, or it may continue until the system determines that the action has ended.

How Is Data Collected?

If the vehicle has an EDR, then its crash data can be downloaded by using a Crash Data Retrieval (CDR) interface. The only commercially available system comes from Vetronix Inc., a wholly owned subsidiary of Robert Bosch GmBH, and licensed by General Motors (GM), Ford and Chrysler. Some joint venture vehicle lines like Isuzu (GM) and Volvo (Ford) also are compatible, but it's important to know that, even with these automakers, not all models can be accessed through

Continued on page 12

'Silent' Passenger

The Auto Black Box Today and in the Future

Continued from page 11

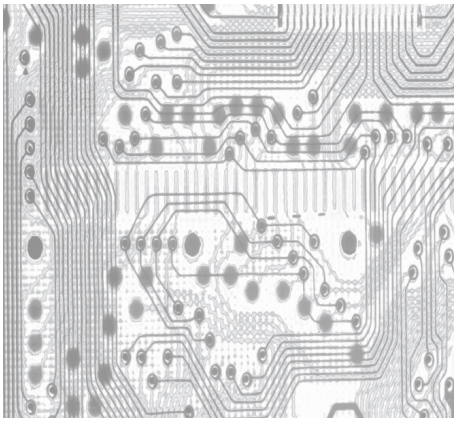
the Vetronix CDR. EDR access for all other automaker models must be initiated through the manufacturers, although they'll now have to facilitate CDR access under the NHTSA rule. Most importantly, CDR downloads are best performed by those trained to operate the interfaces — this could be the automaker, law enforcement personnel or auto accident investigators.

More on the EDR

With the EDR, there are several key points to keep in mind. Tampering with airbag sensors or attempting to remove the EDR can imperil safe operation of the airbags and related safety systems, nullify warranties, and abrogate NHTSA safety standards — and should be avoided at all costs. All the EDR matters should be handled by trained personnel.

At present, there are no guarantees for airbag EDR data accuracy and completeness, and there are operational and structural issues that hamper the technology. For example, automotive black boxes aren't as resilient as their aviation cousins — those can withstand concussion, freezing temperatures, infernos and submersion. Airbag EDRs experience glitches, spotty recording and other challenges, especially as automakers adjust the technology to suit regulators. As a result, the data retrieved from an EDR download is best used as an adjunct to a thorough accident investigation, and virtually never as stand-alone testimony as to facts. Certainly, the data may corroborate claimant statements, but then again, when the issues in question are gray rather than black and white, it is crucial that the evidence be as accurate and as indisputable as possible. The EDR is getting there, but it hasn't arrived yet. Thus, the analysis and interpretation of the data is best left to skilled automotive accident investigators who are aware of the EDR's limitations and are schooled in broader analytics.

The airbag EDR is only one example of a vehicular data-gathering module. Today's



automobiles, especially luxury cars, are networks on wheels — newer models average 17 microprocessors onboard. However, current media attention and regulatory action are directed mainly to the EDR modules embedded in airbag safety systems.

Consumer vs. Carrier

Those who investigate vehicular accidents tend to shrug their shoulders about the fears of privacy invasion. To them, EDR data is akin to any other piece of objective evidence picked up at an accident scene. Law enforcement personnel usually check the brake lights, seatbelts, tire pressures, turn indicators, and more, of the affected vehicles at accident scenes. If they are trained and equipped with a CDR, and the vehicle has an accessible and undamaged system, then they'll download the data, typically with the permission of the vehicle owner. In their world, EDR data is evidence to collect, nothing more.

Things get a little more complicated for consumers. There's something uncomfortable about the chance of being unfairly condemned by a technology deemed infallible. Plus, consumers wonder why they don't get a choice in the matter of the placement of EDRs in their cars. The EDR is not 100 percent accurate, and data can be misinterpreted; but consumers typically don't have the know-how to question its veracity. Thus, fear of a loss of control stimulates the issue of EDR privacy invasion and has typically been the impetus for state and regulatory action about EDR data ownership. Ultimately, the privacy issue boils down to questions of consent: Do you know if your car has an EDR and do you consent to a data download after an accident?

The EDR perspective is a little different for insurance carriers. Its data can deliver certainty to the resolution of some automotive claims. For example, in a fatal accident on an empty nighttime road, the data from a download can reveal facts when there are no witnesses. That's an extreme example, but evidence that adds clarity is invaluable to those who calculate exposures: Absolute answers protect reserves. At least for carriers, the privacy issue associated with data ownership dissipates when carriers assume the ownership rights of totaled vehicles. On the downside, though, ownership of totaled vehicles, as well as complex automotive litigation incorporating EDR data, can expose the carrier to new types of risk. Should the carrier download EDR data as a routine measure, and should the carrier remove and store all EDR modules under its control as a matter of policy? Evidence spoliation risk and a new cost stream associated with long-term storage are unforeseen consequences of harnessing a new technology for automotive claims resolution.

EDRs and the Court

Courts are currently admitting EDR data into proceedings, and appellate courts are upholding its use as well across the U.S. So far, the preponderant users of the data are automakers and criminal courts. Both are tech-savvy about the EDR and know how to use the information in the courtroom — automakers design and build them, and law-enforcement personnel are trained in crash data retrieval. This skewed usage should even out as more parties become familiar with the technology and so, too, will the balance of civil to criminal actions using EDR data as evidence.

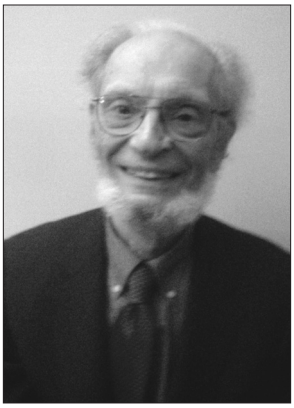
Invasion of Privacy Protection

Privacy protection has been a hot button EDR issue for state legislatures and has also affected the EDR strategy of federal agencies with transportation oversight. As of early 2008, 12 state legislatures have passed some form of EDR legislation. A leader in privacy-rights protection, California addresses the EDR's privacy implications by requiring automakers to disclose to new-car buyers the presence of an EDR in occupant protection systems, and to prohibit the downloading of the data without car-owner consent. Other states restrict regulatory focus to a single EDR issue like disclosure or EDR access. At the national level, the August 2006 EDR rule published by the NHTSA requires automakers to disclose the presence of an EDR to car buyers, starting with model year 2011 cars. And, when the NHTSA and others use EDR data for research purposes, the derived data is purged of all identifiers for the sake of privacy.

The consumer mantra for the EDR is that the owner of the car owns the data. Although that works well enough for now in most states, especially with federal support from the NHTSA and the Federal Highway Administration, that perspective may face challenges as EDR use expands. ■

Spear-Phishing

by Jerome Trupin, CPCU, CLU, ChFC



Jerome Trupin, CPCU, CLU, ChFC, is a partner in Trupin Insurance Services, located in Briarcliff Manor, N.Y. As an "outsourced risk manager," he provides property-casualty insurance consulting advice to commercial, nonprofit and governmental entities. Trupin regularly writes articles on insurance topics for industry publications and is the co-author of several insurance textbooks published by the AICPCU/IIA. Trupin has been an expert witness in numerous cases involving insurance policy coverage disputes, has spoken on insurance topics across the country, and has taught many CPCU and IIA courses. He can be reached at cpcuwest@aol.com.

Spear-phishing isn't the name of a sport for phonetically-challenged scuba divers; it's a refinement on the all-too-common Internet blight known as "phishing." A phisher casts a wide net; a spear-phisher sends a message directly to a specific recipient. (It's easy to get e-mail addresses of people in, for example, the finance department of a large corporation, either by bribing an employee for a list or searching for names on the Internet and then formatting their e-mail addresses using the firm's standard e-mail name-format.) An actual spear-phishing loss occurred as follows:

> Late on a Friday afternoon, Sue Mark (name changed), an employee in the finance department of a large firm, received an e-mail, addressed directly to her, appearing to be from the firm's bank. The message said that there had been a number of unsuccessful attempts to log in to the firm's bank account and directed Sue to the bank's Web site.
>
> The Web site appeared to be legitimate. It asked that she send a reply message containing the firm's bank account number and password. According to the message, this information was needed so the bank could be sure that she was someone in the firm rather than the person attempting to access the account. The message said that the bank would then change the password and let her know the new one. The Web site appeared identical to the bank's actual Web site. It was, of course, run by the spear-phisher. Sue took the bait, and by Monday morning the spear-phisher had withdrawn $650,000 from the firm's bank account.[1]
>
> Could the firm collect for the $650,000 loss under its employee fidelity coverage? Is there any other crime coverage that might apply?

There are two basic types of employee fidelity coverage available today. The Insurance Services Office (ISO) and some other insurers provide what's known as "employee theft" coverage. Employee theft is, logically, a theft by an employee. Theft is defined as "unlawful taking to the deprivation of the insured." In order to trigger coverage, Sue's act would have to be unlawful and she would have to be the one who had done the "taking." Because her actions do not meet that standard, there's no coverage. Sending the account number and password was stupid, but probably not illegal. If stupid acts were illegal, we'd probably all be indicted at one time or another.

The other type of employee fidelity coverage is known as "employee dishonesty." The American Association of Insurance Services (AAIS) and the Surety & Fidelity Association of America (SFAA) make employee dishonesty forms available, as do some independent insurers; at one time ISO offered employee dishonesty coverage. The basic requirement under these forms is that the employee's act be dishonest, not necessarily unlawful. Employee dishonesty forms, however, contain what's referred to as a "dual trigger." The dual trigger requires that the employee

manifest an intent to cause the insured to sustain loss and obtain financial benefit for the employee or another person whom the employee designates. The benefit must be something other than salaries, commissions, bonuses, promotions, profit sharing, etc. Since Sue didn't intend to cause a loss to her employer and since she didn't expect any financial benefit, there's no coverage under employee dishonesty coverage either.

It appears that Sue's employer would also be unsuccessful in seeking coverage under its employee fidelity insurance, whichever form (employee theft or employee dishonesty) is used. Is there a coverage that might apply?

There is coverage available under an ISO coverage known as "Computer Fraud." The computer fraud insuring agreement reads as follows:

> **6. Computer Fraud**
> We will pay for loss of or damage to "money," "securities" and "other property" resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the "premises" or "banking premises":
>
> a. To a person (other than a "messenger") outside those "premises;" or
>
> b. To a place outside those "premises."[2]

This appears to be a coverage that would protect Sue's firm. We don't know exactly how the spear-phisher obtained the funds. Depending on the exact way that the spear-phisher communicated with the bank, coverage might be found under ISO Crime Funds Transfer Fraud coverage instead. It reads as follows:

> **7. Funds Transfer Fraud**
> We will pay for loss of "funds" resulting directly from a "fraudulent instruction" directing a financial institution to transfer, pay or deliver "funds" from your "transfer account." "Fraudulent instruction" means: An electronic, telegraphic, cable, teletype, telefacsimile or telephone instruction which purports to have been transmitted by you, but which was in fact fraudulently transmitted by someone else.[3]

Because it recognizes the possible overlap between these coverages, the ISO Computer Fraud coverage form excludes any claim that qualifies as Fund Transfer Fraud claim and the Fund Transfer Fraud coverage excludes any claim that qualifies as Computer Fraud. To avoid this overlap, some insurers combine the two coverages into one insuring agreement.

Spear-phishing may be the most exotic, but it's far from the only way that criminals can help themselves to a firm's bank account. A front page story by **John Markoff** in the Dec. 5, 2008, issue of *The New York Times* starts out: "Internet security is broken, and nobody seems to know quite how to fix it." The story goes on to point out that credit card thefts, bank fraud and other scams rob computer users of an estimated $100 billion a year. Amazingly, the author writes that "a Russian company that sells fake antivirus software that actually takes over a computer pays its illicit distributors as much as $5 million a year."[4]

The most common source of computer and fund transfer fraud losses are employees. The CFO of the American Cancer Society's Columbus, Ohio, office, who had wired $7 million from the Cancer Society's bank account to one in his name in an Austrian bank, was arrested just as he was boarding a plan to flee the country. An employee's thefts would be covered under fidelity coverage — another argument for high limits for that coverage. But the Internet has given criminals worldwide the opportunity to invade a firm's bank accounts. To protect against those losses, Computer Fraud and Fund Transfer Fraud coverages with high limits are vital for virtually every enterprise. ■

References

1. Based on a presentation by George N. Allport, Chubb Insurance, at the Westchester CPCU Chapter/Westchester Community College seminar on Nov. 21, 2008.
2. ISO Properties Inc., CR 00 20 05 06 Commercial Crime Coverage Form © 2005.
3. ISO Properties Inc., op. cit.
4. Markoff, John. "Thieves Winning Online War, Maybe Even in Your Computer. "The New York Times: Dec. 5, 2008.

CPCU Society
INSURING YOUR SUCCESS

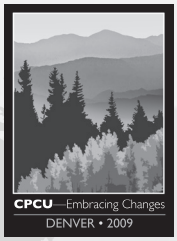
Information Technology Interest Group

Volume 16 • Number 2 • August 2009

Cutting Edge

CPCU Society
720 Providence Road
Malvern, PA 19355
www.cpcusociety.org

Address Service Requested



Explore the Ways to Embrace Change in Denver!

Attend the CPCU Society's Annual Meeting and Seminars

Aug. 29–Sept. 1, 2009 • Denver, Colo.

In today's economy, it's more important than ever to continue to build your skills and your network, and to be fully prepared to seize new business and career opportunities.

- **Be Inspired to Keep a Positive Focus.**
  Celebrate with the CPCU Class of 2009 at the AICPCU Conferment Ceremony and hear the dramatic survival story of Colorado mountaineer, author and survivalist **Aron Ralston.**

- **Learn How to Maximize Resources.**
  Attend the keynote address, "See First, Understand First, Act First — Leadership and Preparedness in the 21st Century," by **Lt. General Russel Honoré,** U.S. Army (Ret.), who led the Hurricane Katrina military relief efforts.

- **Sharpen Your Competitive Edge.**
  Expand your knowledge base with an all-new lineup of more than 45 technical, leadership and career development seminars.

- **Identify Industry Trends.**
  Glean inside perspectives on diversity and international issues from industry leaders at two new General Sessions.

Register today! For details, visit **www.cpcusociety.org.**

The Information Technology Interest Group newsletter is published by the Information Technology Interest Group of the CPCU Society.

Information Technology Interest Group
http://infotech.cpcusociety.org