RMQ

Risk Management Section Quarterly

Vol. 19 No. 1
April 2002

CPCU SOCIETY
INSURING YOUR SUCCESS

Cell Phones and Driving—One Risk Manager's View

by D. Theodore Flores Jr., CPCU, ARM

I was sitting at a stop sign the other day, watching helplessly as a car approached from behind without slowing. As the car came closer I could see that the driver had her head turned toward the back seat and she was dealing with a young child in a car seat. Fortunately for me, she turned around in time to slam on the brakes and stop without hitting me.

This "near miss" incident got me thinking about the extraordinary amount of attention that has recently been focussed on drivers using cell phones. Much of this attention has been triggered by a recent wrongful death lawsuit filed in Virginia against a law firm. An associate of the firm was on her way home at 10 p.m. when, while allegedly making business calls on a cell phone, she accidentally swerved off the road and struck and killed a pedestrian.

The significance here is that the employer may be held responsible because of the alleged **business use** of the cell phone at a time (coming to/going from work) when it previously had no exposure. Had this accident occurred while the employee was on her way to the office of a client or to the courthouse, the employer could have been held liable anyway, phone use or not. Therefore, it is the time of the cell phone use and not the use per se that creates a new exposure for the employer. If this allegation against the employer holds, then use of a cell phone to make business calls while on the way to or from work could bring commuting within the course and scope of employment. There could also then be workers compensation ramifications.

In response to this case, a number of my colleagues have recommended the implementation of corporate policies prohibiting the use of cell phones while driving. As a risk manager and cell phone user (yes, while driving), I am not convinced that cell phone use materially increases the risk of an auto accident any more than a host of other distracting activities a driver can engage in, i.e. the inattentive driver referenced above. If cell phone use while driving is prohibited, why not prohibit eating and drinking while driving? A driver's attention to the road can certainly be diverted when a drop of ketchup falls from a burger onto his or her shirt, or while wrestling that last french fry out of the fast food bag. Smoking while driving must also be considered a safety hazard. Isn't the act of reaching into a glove box for a pack of cigarettes, pulling one from the pack and lighting it as dangerous as talking on a cell phone? Trying to locate and count tollway change is hazardous, as is changing compact discs while driving. Even the act of talking with a passenger can divert a driver's attention from the road. I am sure the list of unsafe acts committed by drivers is endless.

How should an employer respond to this issue? There are a number of pitfalls associated with the implementation of a company policy to either prohibit cell phone use while driving or requiring drivers to pull over and stop their car before using a cell phone. As near as I can tell, most people concede that these policies will be unenforceable, but are being put in place to reduce the possibility of a punitive damage award.

- Penalties for violating the company policy must be determined. What is reasonable punishment for using a cell phone while driving?
- The problem of equal enforcement of penalties can be problematic. Is the company prepared to deal with a violation by its CEO in the same way it deals with a violation by a salesperson?
- If an employer has a policy but fails to enforce it, has a punitive damages exposure now been created? The same consequences could be true in a case involving a repeat offender. In my experience, a policy unenforced can be more harmful than no policy at all.

I also do not believe that a driver's violation of a company's cell phone use policy necessarily creates a corporate veil. Legal scholars can debate me on this point, but I believe a court will impute liability to an employer for the negligence of its employee where an auto accident occurs in the course and scope of employment, whether or not cell phone use is the cause. When all is said and done, the only practical result of a phone use policy may be to limit an employer's liability when an accident resulting from business cell phone use occurs during non-business hours (i.e. commuting).

It may be that state or federal governments will save us all from this dilemma by enacting legislation prohibiting drivers from using cell phones while operating a moving vehicle (I am told New York already has done this.) If governments don't make an attempt to control this, will commercial auto insurers require a company to have a cell phone policy as a condition for underwriting the business?

Driving an automobile simply requires the use of good judgment, all the time. Additional legislation or work rules will not assure that good judgment is exercised. If you would like to challenge or comment on this opinion, please direct your response to the *RMQ* editor or me. ■

D. Theodore Flores Jr., CPCU, ARM, is corporate risk manager for Griffith Laboratories International Inc. and a member and former chairman of the Risk Management Section Committee.

Accidents Don't Have to Happen

by Jerry Goldman, LC

It's a peaceful summer evening. As the sun sets, an elderly woman makes her way across a parking lot to her car. Suddenly she slips causing injury. Hello, lawsuit.

We've all heard the story before. As a lighting professional and expert litigation witness, I never fail to be amazed at the lack of safe outdoor lighting I see in the parking lots of so many of today's buildings. Especially when it's so easy to avoid injuries—and the claims that follow them—with a simple check to make sure the lighting is up to code.

You might think all you need for complete parking lot safety are dozens of bright floodlights. Unfortunately, it's not that simple. While some lots are far too dark to be safe at night, many others offer areas that are bright enough to create unsafe glare or variations in lighting levels that can lead to temporary blindness, particularly in the elderly.

But there are answers out there.

Since about 1995, many municipalities across the United States have realized there is a relationship between lighting and safety. A direct result has been the proliferation of lighting codes. In South Florida, where I live and work, all but a handful of cities and counties now have very specific codes that deal with lighting as it affects public safety. These codes apply to all commercial properties and residential properties of four dwellings or greater. But less than 5 percent of South Florida properties built before 1997 has had lighting upgrades and doesn't meet the newer requirements.

Even many newer properties aren't up to code. Although the design engineer may have satisfied all lighting code requirements, poor maintenance often causes the property to be non-compliant with local code. Since few municipalities require ongoing lighting inspections, property owners don't know they're vulnerable to injury claims until it's too late.

And that can be an expensive surprise.

But what if you had a way of quantifying levels of safety in the properties you underwrite? Just like the auto insurance industry offers rewards for careful drivers, safer cars, and theft prevention devices, doesn't it make sense to offer financial incentives for properties that can prove they've limited their liability?

There are straightforward equations that can be applied to any property that describe the safety factor of an illuminated area. Most municipalities get their information on lighting levels from the Illuminating Engineering Society of North America (IESNA). This organization of electrical engineers and lighting designers sets standard guidelines for every imaginable type of lighting. It sponsors ongoing research to define and improve lighting standards as technology changes every lighting category.

The lighting of parking lots is just one area IESNA has been studying. The IESNA supports any municipality that considers an adjustment to its lighting codes and helps policymakers obtain the most up-to-date and accurate information.

The information being developed by IESNA is already making parking lots safer all over the country. Soon, that same information will become an invaluable tool for underwriters too. ■

Jerry Goldman, LC, has worked in the lighting industry for more than 30 years. During that time, he has participated in many changes that have made today's lighting more functional and energy efficient.

Goldman's LC credentials were awarded by "The National Council on the Qualification for the Lighting Professional." This organization, founded by the U.S. Department of Energy, the Environmental Protection Agency, the General Services Administration, and the Illumination Engineering Society of North America, identifies and certifies the country's foremost lighting experts to promote safe, effective, and efficient lighting practices.

Goldman is available for consultations. He can be reached by phone at (305) 653-0701 or by e-mail at Jerry_D_Goldman@MSN.com. He welcomes any questions or comments you may have.

Member Spotlight

Steven Pahl, CPCU, ARM, is executive director of the Gongaware Center at Indiana State University. Steve has enjoyed a distinguished career in the property and casualty insurance industry spanning 23 years. During that time he held executive management positions with leading insurance underwriting, third-party administration, and retail brokerage firms.

Steve is past chairman of the Risk Management Section of the CPCU Society and, for three years, editor of the *Risk Management Quarterly*. He holds both the CPCU and ARM designations, a B.S. from DePaul University and an M.B.A. from Loyola University of Chicago.

When asked why he joined the Risk Management Section, Steve replied, ". . . because it represents, for me, the sum of all the individual disciplines that the other sections represent, focused in a problem-solving manner. The risk management process still represents the best known methodology for dealing with the myriad of new risks that emerge from the global economy almost on a daily basis." ■

Internet Revolution—World Wide War

by Peter R. Taffae

Peter R. Taffae is president and CEO of e-perils.com™, a division of Worldwide Facilities, Inc., specializing in Cyber, D&O, EPLI, Crime, and E&O insurance for corporate and financial institutions. He can be reached at (213) 251-2427 or PeterT@eperils.com.

Over 40 years ago, Che Guevara, Fidel Castro, and Camilo Cienfuegos came marching down from the Sierra Maestra Mountains into Havana and ousted President Batista. The rest is history. Castro has ruled Cuba ever since. In 1949 it was guns and political outrage; today's wars are being raged on the Internet. Are today's Gates, Cases, and Linus Torvalds yesterday's Ches, Castros, and Camilos? Did anyone anticipate the Internet Revolution would include political revolutions?

This new high-technology revolution is not only occurring in the country of Cuba but recently in China, Kosovo, East Timor, and the Middle East. This is the beginning of a new era in rebellions.

These new rebels are known as Internet guerrillas. They represent the new resistance to governments in power via the Internet. Internet guerrillas' attacks have resulted in e-mail flooding, denial of service attacks, and hacking of web sites worldwide. Often the guerrillas test their abilities on innocent targets first via third-party servers as relays for their attacks. This results in legal liability for those innocent servers and web sites. The most vulnerable to these malicious attacks are small and mid-size companies that cannot afford to employ the personnel that have the necessary security experience to halt these attacks. There are already many examples of American universities and commercial sites that have been used as third-party conduits.

The fact that information is freely exchanged globally at little or no cost has allowed and even encouraged opposing parties to dissimulate and gather, sometimes, secretive information to assist their causes. In some countries, and Cuba in particular, the Internet threatens the government's control of information. Its monopoly of information is now being challenged. War is won via information and there is no easier, quicker, and less expensive information then the Internet has to offer. **Some compare today's Internet guerrillas to World War II's French resistance role in war.**

In Cuba, the state-owned news agency distributes information that it feels is relevant to the people of the country. The idea of someone being able to log onto CNN's web site and see the world contradicts the monopoly that the government has had all these years. The Internet is uncontrollable, which is exactly why it can easily crumble the leaders of a controlled environment. For the very reason the Internet has led the developed countries into a new economy, the speed and efficiencies of the Internet will play a larger and larger role in developing countries' political environments.

In late December, China made it a crime to use the Internet as a way to further Taiwan's independence. China has said it will attack Taiwan if the island declares its independence since the civil war of 1949 when the island became a breakaway province. The Standing Committee of the National People's Congress passed a resolution stating, among other things, that spreading computer viruses and breaking into national defense networks are criminal activities. Many of the resolutions' "new" laws mirror existing laws that are used to arrest dissidents and members of opposing political groups but for the first time the Congress addressed "criminal activities" specifically arising out of the Internet.

Recently, across the globe from Cuba and China, in the Middle East we have seen how the Internet is being used to further opposing political views. The Anti-Defamation League web site was attacked the end of December by anti-Israeli Internet guerrillas. The site was taken over for about 30 minutes where the attackers posted threats to Israelis and other pro-Palestinian opinions. Other sites that have been hit by Internet guerrillas include: Bank of Israel, the Tel Aviv Exchange Market, Palestinian National Authority, and the Palestinians Hamas' site.

As recently as mid-January 2001, hackers calling themselves Pentaguard hit a series of Australian, U.S., and UK government web sites. These sites were replaced with home pages and links with Pentaguard's logo. **Pentaguard is believed to be based in the United States and claims to be running a World Wide Web War (WWW).** Many security experts believe that if groups like Pentaguard can break into a government site with such ease then commercial sites are very accessible to unauthorized access.

The FBI has issued a warning to the U.S. government and corporate America that their web sites are potential targets from Internet guerrillas.

> Based on FBI investigations and other information, the NIPC has observed that there has recently been an increase in hacker activity specifically targeting U.S. systems associated with e-commerce and other Internet-hosted sites. (www.nipc.gov)

It is important to understand any companies with sales to clients based in the Internet war territories are vulnerable to cyberattacks. Already there have been reported incidents with U.S. firms conducting business in Israel being hacked. Many of

Continued on page 4

Internet Revolution—World Wide War

Continued from page 3

these attacks will come via innocent third parties. By using "conduits," hackers disguise their identity and make capture almost impossible. One good example of an innocent third party involved was the denial of service attacks on some of the largest B2C web sites on February 9, 2000, when the University of California at Santa Barbara was covertly used as a conduit for the attacks.

At the end of the day there are no measures that can stop all politically motivated Internet warfare. **Governments as well as companies are wrestling with how to protect their technology boundaries.** For now, there are a few steps corporations need to take to minimize their veniality and protect themselves from Internet guerrillas.

Every company with an Internet presence should seriously consider a comprehensive security assessment. The level of assessments can be tailored to a firm's financial budget. It is an excellent process because of the diversity of issues/concerns that will be addressed.

Equally important is cyberinsurance to protect senior management and the company's balance sheet. The perils arising from the Internet need to be addressed, as are the traditional perils of fire, flood, etc. **There are a number of insurance contracts that have been specifically designed to protect against the numerous perils arising out of the World Wide Web.** Knowing the good ones from the bad is the trick in this ever-changing, quick-moving environment. ■

Risk Management Section Quarterly
is published four times a year by and for the members of the CPCU Society's Risk Management Section.

Editor
Kathleen A. Murphy, CPCU
murphys.kandb@attbi.com

Section Chairman
George J. Kolczun Jr., CPCU
Rooney Insurance Agency
5601 S. 122nd E. Ave.
Tulsa, OK 74146

Sections Manager
John Kelly, CPCU, ARM, AAI
CPCU Society

Managing Editor
Michele A. Leps
CPCU Society

Production Editor
Joan Satchell
CPCU Society

Design
Susan Chesis
CPCU Society

CPCU Society
Kahler Hall
720 Providence Road
PO Box 3009
Malvern, PA 19355-0709
(800) 932-2728
www.cpcusociety.org

Send articles and letters to:
Kathleen A. Murphy, CPCU
c/o CPCU Society
720 Providence Road
PO Box 3009
Malvern, PA 19355-0709
www.cpcusociety.org

* denotes home address

RMQ

CPCU SOCIETY
INSURING YOUR SUCCESS

720 Providence Road
PO Box 3009
Malvern, PA 19355-0709

Risk Management Section Quarterly

Vol. 19 No. 1
April 2002

PRSRT STD
U.S. POSTAGE
PAID
BARTON & COONEY