

The Eyes Have It  
CSI March 2004 Alert  
Rebecca Herold, CISSP, CISM, CISA, FLMI  
January, 2004

While at a recent ISACA meeting, I was engaged in a brief but enlightening and disconcerting conversation with a group of the attendees about camera cell phones. One of those present became clearly disgusted with the conversation and stated, "There are no risks involved with camera cell phones in businesses. You could never be able to interpret any writing on papers you take photos of with those things!" Then he quickly switched the conversation. Interesting. How many other business leaders also share this same point of view and dismiss the issues involved?

A few days prior to the meeting a new Iowa bill was introduced on January 15, 2004. House File 2037 would make it a criminal offense to use a camera cell phone in areas "where another person has a reasonable expectation of privacy." A violation would be a simple misdemeanor, with a fine of \$100. Iowa is not the only state concerned with camera phones.

Have you thought about the business ramifications of camera phones and the impacts of existing and emerging laws?

**What's to Worry About?**

There are huge numbers of camera cell phones all around us. According to In-Stat/MDR, 43.3 million cell phones had cameras in 2003, and they project there will be 366 million camera cell phones by 2008. As the numbers of camera cell phones proliferate, so do the camera cell phone incidents. Here are a few of many reports related to camera phone use:

- Reported February 6, 2004, WashingtonPost.com: Camera cell phones are not allowed within Air Force facilities that handle classified information. The ban applies across the Air Force. Offices were notified that persons who bring camera phones into restricted areas "could have them confiscated and could face federal charges."
- Reported Tuesday, February 3, 2004, Seattle, WA, Seattle Post Intelligencer: A man who slid his cell phone camera under a woman's skirt as she pushed her baby at a local store pleaded guilty to one count of voyeurism. He will be sentenced March 19, facing up to five years in jail, up to \$10,000 in fines, or a combination of both.
- Reported February 2, 2004, Mountain Home, Arkansas, BaxterBulletin.com: In an article from the sheriff's office, Sergeant Tim Phillips reports the use of camera phones by criminals has increased identity theft crimes in some areas by as much as 20%. He goes on to discuss how criminals accomplish this by taking photos of credit cards as consumers use them to pay for purchases in stores.
- Reported January 17, 2004, Poughkeepsie Journal: All Sport in Poughkeepsie forbids members from using cell phones in the workout areas and encourages people who need to make calls to handle them in the lobby. In August, a 15-year-old New Jersey boy used his camera phone to capture the license plate of a man who had pulled over and tried to kidnap him. Police arrested the man a short time later.
- Reported January 8, 2004, North Adams, NH, Associate Press: The local YMCA banned camera cell phones from the locker room because of privacy concerns. Hampshire Regional YMCA is reported likely to follow suit. The Chicago-based YMCA of the USA recommended in June that its 2,500 independent branches ban camera phones, even though there had been no improper use incidents reported. YMCAs in Kansas, Maryland and Wisconsin have banned the use of camera cell phones in locker rooms.

The Eyes Have It  
CSI March 2004 Alert  
Rebecca Herold, CISSP, CISM, CISA, FLMI  
January, 2004

- Reported December 30, 2003, Des Moines, Iowa, [theiowachannel.com](http://theiowachannel.com): Oakmoor Racquet & Fitness banned cell phones in locker rooms to help protect privacy.
- Reported July 5, 2003, The Korea Herald: Samsung Electronics banned the use of camera cell phones in its research facilities because of fears that competitors could obtain competitive information using them.
- Reported October 20, 2003, Sun Prairie Wisconsin, Associate Press: Prairie Athletic Club has banned camera cell phones in locker rooms because of privacy concerns. Wisconsin state Rep. Marlin Schneider indicates posting a picture on the Internet taken with a cell phone could be considered invasion of privacy, and could result in up to 3.5 years in prison and a \$10,000 fine.
- Reported September 9, 2002, Tokyo, The International Herald Tribune: Widely reported uses of the camera phones to secretly shoot under women's skirts in public areas such as train stations. First time offenders face a fine of as much as \$4,250 or six months in jail. In another case two junior high school students used camera phones to take pictures of a naked classmate in the locker room and threatened to post to the Internet.

Web sites are emerging that look in depth at the issues involved with using camera phones. For example, the following are just a few of the interesting tidbits from [cameraphonereport.com](http://cameraphonereport.com):

- "Criminals being arrested because their photos were sent to the police by citizens. (One example: A teenager was solicited by a man in a car. The teenager took a photo of the man and the license plate. The teenager went to the police and the man was arrested the next day.)"
- "Camera phones already are being employed in "vertical markets": Construction workers sending photos to supervisors to get advice about construction problems; real estate agents sending photos to clients about new homes on the market; car salespeople attending automobile auctions sending photos to their bosses and potential purchasers of autos."
- "Women in Japan are taking photos of their taxi drivers to help ensure that nothing "untoward" occurs -- and ensuring they have a record if something does occur."
- "Emergency personnel are transmitting photos of accidents to hospitals to get advice about how to handle situations."
- "Doctors are using cellular phones to transmit X-rays to other doctors for consultations."

Another site, [picturephoning.com](http://picturephoning.com), also contains interesting and useful information about camera phones. Here are a few of the notes from that site:

- "In the same field, a company, RealSafe.net Network, is suggesting real estate agents use their camera phones - not to shoot property - but to snap pictures of their clients (with their permission), as a form of insurance and store in a secure database, which can only be accessed by court order. "

The Eyes Have It  
CSI March 2004 Alert  
Rebecca Herold, CISSP, CISM, CISA, FLMI  
January, 2004

- "A contractor in the business of sealing driveways, has been taking pictures of any pre-existing tar splatters on a customer's garage or house. "Just so if a customer asks, I can say, "Here, look, that was there before I started." "
- "Adrian Contreras of San Mateo, saved himself a San Francisco parking ticket by "phone-ographing" his correctly placed wheels after receiving a citation for not turning them toward the curb. And the city accepted the photo as proof."
- "The Malaysian police and the Australian government have set up systems to monitor picture messages sent in by citizens reporting crimes."
- "And camera phones have brought about the onset of a whole new form of online diaries, called photoblogs, where camera phone users can post their pictures while on the move. Mostly of a personal nature, next year is sure to see a widespread use of professional moblogs, such as Textamerica's launch of the official moblog for the CTIA event held in Las Vegas or news reporting photoblogs such as those documenting the New York blackout, the anti war protests around the world, the California fire, The California grocery worker strike - all reaching a larger audience than just family and friends."

#### **Laws and Regulations**

The proposed Iowa law banning camera phones is not the only camera phone related law being considered.

- Reported in Cleveland, Ohio, October 13, 2003, whiotv.com: David Bentkowski, Seven Hills council member, wants legislation to ban camera cell phones from areas in the city, such as public restrooms, health clubs and recreation centers, as a precaution to protect personal privacy. He's pushing for legislation that bans camera cell phones from areas in the city that can jeopardize someone's privacy -- like in health clubs, recreation centers, and public restrooms.
- Reported November 17, 2003 in the Wisconsin State Journal: A recently passed law makes it a criminal misdemeanor to look into private places, including showers and dressing rooms. This applies to the use of camera phones.
- Reported November 25, 2003, Newark, NJ, Newark Star-Ledger: The use of camera phones prompted a new bill, approved by the New Jersey Senate Judiciary Committee, that would make it illegal to secretly view or videotape anyone in a private location where people undress or engage in private activities.
- Reported November 17, 2003, Seoul, South Korea, BNA: The Ministry of Information and Communication has issued requirements to make camera cell phone cameras more privacy-sensitive. Rules announced November 11 require all new camera cell phones produced to make a loud (65 or more decibels) sound, such as a loud shutter click, or a human-like voice, whenever a photo is taken. This feature must not be able to be disabled. The rules do not apply to phones already being used, or to phones sold in markets outside South Korea.
- Reported August, 2002, South Korea: Bill number 162568, would make photographing people against their wishes, by any devices including camera phones, punishable under criminal law. The bill is awaiting parliamentary review by the National Assembly.
- Reported October 1, 2002, silicon.com: Saudi Arabia banned camera phones because they had been, and could be, used to secretly photograph women.

The Eyes Have It  
CSI March 2004 Alert  
Rebecca Herold, CISSP, CISM, CISA, FLMI  
January, 2004

- California has a voyeurism law, S647(k)(1) of California's Penal Code, that covers camera phone abuses.
- Section 9A.44.115 of the Revised Code of Washington covers camera phone abuses. It classifies voyeurism as a felony that occurs when a person photographs another person without the person's knowledge and consent where they would expect privacy.

### **Risks Within Organizations**

It is probably unrealistic to ban the use of camera phones completely within your organization; this may soon be analogous to banning all cell phones. With our dependency upon cell phones to communicate to perform business, and the use of cell phone numbers as our primary business numbers, this is not feasible. In fact, there may be activities within your organization where the use of camera phones will benefit your business processing. You need to look at the risks involved with camera phones in your organization, industry, locations and jurisdictions and establish the policies and controls necessary to diligently address the risks. When making such policy and control considerations, don't forget to consider regulations, such as HIPAA and GLB, that apply to your organization. For example, what precautions do you need to establish for protected health information (PHI) to ensure you are complying with Privacy Rules in areas such as patient care rooms and meeting rooms where PHI is discussed? Document your risk identification process, and implement controls that demonstrate your organization's due diligence in protecting customer and employee privacy.

Here are some camera phone related issues to help you start identifying your risks. Some of these may be of great importance in some organizations, and not applicable at all in others.

- Taking photos in locker rooms, restrooms, and other areas where privacy is expected.
- Covertly photographing classified company information and trade secrets and sending it to competitor. This presents more risk than traditional methods of stealing trade secrets because of the speed with which such information can be sent to the Internet or to someone else, and the lack of tools to detect such activities.
- Snapping embarrassing photos at the company-sponsored functions and then posting them on websites or using them for extortion.
- Possible hostile work environment claims that may occur from photos being taken, or allowing photos to be taken, of personnel without their consent.
- Photographing personnel credit cards while they are traveling or making purchases on the behalf of your company.
- After the images and information is posted to the Internet it is virtually impossible to withdraw the information from uncontrolled circulation. No matter what type of legal court order you obtain, the information, once posted on the wild Internet, is subject to uncontrolled copying. Once your image has hatched in cyberspace, your chick quickly flies the coop to quickly reproduce and not come back home to roost.
- Used by a terminated personnel to take propriety information to a new employer and possibly competitor.
- Used by a disgruntled employee to harm the organization.

The Eyes Have It  
CSI March 2004 Alert  
Rebecca Herold, CISSP, CISM, CISA, FLMI  
January, 2004

- Used by personnel to document management abuses, safety violations, harassment, and so on. This may be considered a risk or a benefit, depending upon your organization and the motivation of the person taking the photos.
- Sensitive research, trade secrets, merger plans, stock information, and so on, written on white boards, flip charts, and blackboards, might innocently, or purposefully, end up in someone's camera cell phone.

**Controls to Consider**

What options do you have for addressing camera phone risks? Well, of course you could establish a policy to completely ban the use of such devices. However, this will not be feasible for most organizations. On the other hand you probably do not want to allow employees to use camera phones for fun and pleasure while they are at work. Consider camera phone use in ways similar to how you consider the use of handheld computing devices, email communications, Internet access, and similar technology-related business functions. Consider using some of the following controls based upon your business environment:

- Completely ban all camera phones from facilities.
- Ban the use of camera phones in areas where privacy is expected, such as locker rooms and restrooms.
- Require non-employees and visitors to executive offices to check their cell phones with the security guard or personnel who is accompanying them at all times.
- Do not allow third parties to bring camera phones with them into corporate facilities. Require third parties to keep cell phones within a case or container at all times while within the facilities.
- Only allow the use of camera phones that automatically may a very loud noise when photos are taken.
- Do not allow camera phones in areas of advanced research and development, or departments where top-secret or sensitive activities are performed or information is stored.
- Be mindful that digital cameras can also be installed in briefcases or even eyeglasses.
- Consider installing technology in sensitive and privacy areas of your facilities that will disable camera capabilities. Iceberg Systems is one vendor that has such systems.
- Prohibit camera phones in certain business units or departments, such as in the executive offices, laboratories, hospital rooms, and so on.
- Establish policies and procedures to protect personnel PII such as credit card numbers, while traveling or making business purchases.

Occasionally check the sites mentioned earlier, and sites like them, to see what's new in the world of camera phone capabilities, risks and incidents. Re-examine your approach to controlling the use of telephones, cell phones, camera phones, handheld computers, and other new technologies. Review and update your policies with these in mind. Educate your personnel on the appropriate and safe way to use camera phones, and to be aware of others with camera phones when in public. If you don't practice due care to address your

The Eyes Have It  
CSI March 2004 Alert  
Rebecca Herold, CISSP, CISM, CISA, FLMI  
January, 2004

organization's risks from the threats of camera phones, other eyes may end up falling upon your corporate activities and information intelligence.

Rebecca Herold, CISSP, CISM, CISA, FLMI is VP - Privacy Services and CPO for DelCreo, Inc., [www.delcreo.com](http://www.delcreo.com), and can be reached at [rebeccaherold@rebeccaherold.com](mailto:rebeccaherold@rebeccaherold.com) or 515-491-1564. Rebecca has a B.S. in Math and Computer Science, an M.A. in Computer Science and Education, created "The Privacy Papers" and co-authored "The Practical Guide to HIPAA Privacy and Security Compliance" both published by Auerbach and available on [www.amazon.com](http://www.amazon.com).