Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Surviving The Camera Phone Phenomenon

The principal aim of this paper is to present the security practitioner with a compelling argument in favor of the immediate planning and implementation of appropriate security measures to protect against the threat of camera phones. Current organizational security policies which specifically address photography in its various forms will likely prove insufficient or incomplete as camera phones become more ubiquitous, primarily because camera phones possess the ability to electronically distribute images over the Intern...

Copyright SANS Institute
Author Retains Full Rights

AD
nitrosecurity Log Management

Surviving The Camera Phone Phenomenon:
An Analysis of Personal & Corporate Security

Russell Robinson
GSEC Practical v1.4b - Option 1
February 24, 2004

© SANS Institute 2004, As part of the Author retains full rights.

ABSTRACT

The principal aim of this paper is to present the security practitioner with a compelling argument in favor of the immediate planning and implementation of appropriate security measures to protect against the threat of camera phones. Current organizational security policies which specifically address photography in its various forms will likely prove insufficient or incomplete as camera phones become more ubiquitous, with the primary reason being that camera phones possess the ability to electronically distribute images over the Internet moments after they are captured. Thus far in the mainstream media there have been various reports of individuals surreptitiously snapping photographs of unsuspecting subjects in compromising or embarrassing situations, but there has been relatively little mention of the inherent dangers camera phones pose to corporate America. If you are a security practitioner by trade, are responsible for securing your organization's vital assets, or are simply concerned about personal security and/or privacy issues raised by these devices, it is imperative that you be made aware of the various threat vectors and take appropriate action now. This paper will delve into some legal, ethical, and socioeconomic issues surrounding camera phones and their use, and should provide an excellent starting point for drafting security policies.

INTRODUCTION

Modern photography has its earliest roots in a process developed most notably by the French printmaker and painter Louis-Jacques-Mandé Daguerre, who is credited with producing some of the very first photographs in history[1]. The success of Daguerre's invention was swift and widespread, and has since altered the courses of art and science quite dramatically[2]. One of the most significant limitations of Daguerre's technique, however, aside from the lengthy exposure

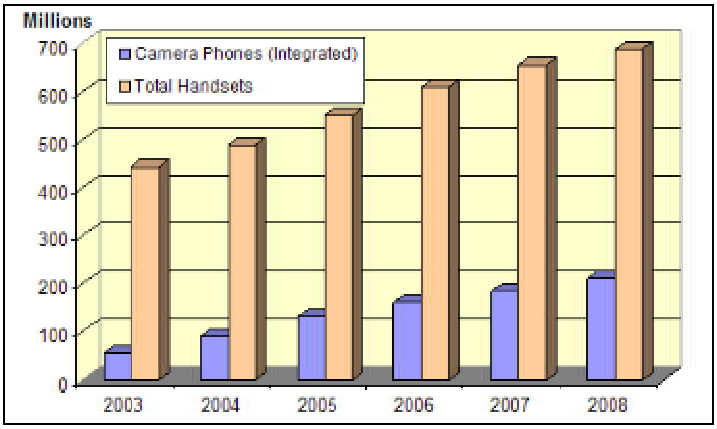
[1] Paraphrased from http://www.rleggat.com/photohistory/history/daguerr.htm
[2] Paraphrased from http://www.metmuseum.org/special/French_Daguerreotypes/dawn_more.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

times, was that objects which were in motion at the moment the photo was taken failed to show up in the final product. Hence, Daguerre's technique proved unsuitable for snapping photos of scenes such as a busy intersection or active wildlife, but it was perfect for taking portraits, since just about anyone could remain sufficiently still during the approximately sixty seconds required for the photo to be exposed[3]. Incidentally, this limitation would have also facilitated a quick escape for anyone not wanting to be photographed—the key was to simply remain moving, whether that entailed bustling about in front of the camera or simply running away.

Nearly two hundred years later, this is clearly not the case. As a result of the many technological quantum leaps which have been achieved in the field of photography since Daguerre's heyday, especially in the realm of digital photography, it is now possible to take pictures of virtually anything or anyone at any given time—regardless of consent. Cameras are faster and more powerful than ever, and feature potentially limitless options for storing, editing, and printing photos with the aid of a computer and printer. As if that weren't enough, camera phones (internet-connected mobile phones with the added ability to capture images and/or video) are a relatively new phenomenon which facilitates the instantaneous transmission of images via email or the World Wide Web, without any need for a computer. Clearly, this unique feature of camera phones carries with it a host of security and privacy issues. This paper will explore some of those issues and provide some useful information to security practitioners concerned about the inherent security threats posed by this new technology.[4]

USAGE STATISTICS



Source: www.3g.co.uk/PR/August2003/5738.htm

Referring to camera phones as being a "new technology", along with their relative unpopularity in the United States may lead some to believe that their use is currently not very widespread. On the contrary, the number of camera phones already in consumers' hands may be somewhat surprising: "An estimated 37 million [camera phones] were sold worldwide last year, according to projections...that's more than double the number sold in 2002."[5] In addition, there is a substantial amount of data which suggests that camera phone usage will see

[3] Daguerreotype exposure time taken from http://memory.loc.gov/ammem/daghtml/dagdag.html
[4] Idea for first two paragraphs (Introduction) gleaned from http://64.177.207.251/CIIMA/CIIMA%20V3%20N110%20Dunphy.pdf
[5] Quoted from http://www.dailyherald.com/search/main_story.asp?intid=38011297

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

some dramatic increases over the next several years. For instance, "Strategy Analytics, an international research and consulting firm specializing in high-tech markets, forecasts that a total of 800 million camera phones worldwide will be sold between 2003 and 2008."[6] A *Wired Magazine* columnist proffers the bold proclamation that "camera phones are well on their way to becoming the most popular consumer device in history."[7] All of this boils down to one simple fact: appropriate security measures need to be put into place **now** to prevent this technology from potentially causing big problems down the road.

SECURITY RESPONSE

Over the course of the past year or so, one of the more common practices employed by organizations that deem camera phones to be a considerable threat is to ban them altogether. While that method will surely put a dent in the number of camera phone-related incidents they'll be forced to deal with, it could also be looked at as a knee-jerk reaction typical of people or organizations when they are faced with unknown risks. Your particular organization may or may not need to institute a ban on camera phones, and the decision will likely hinge on the outcome of a thorough risk assessment. Below are a few examples of fairly drastic measures already taken by several companies in response to the threat of camera phones:

- Intel and General Motors have banned camera phones from their research and development facilities and factories[8]
- Gyms such as Bally Total Fitness and The Sports Club/LA have banned camera phones from all work-out areas[9]
- Employees and visitors at Daimler-Chrysler are not permitted to bring camera phones into any company building[10]
- Employees at Texas Instruments are allowed to bring camera phones into the workplace, but are forbidden to snap any pictures[11]
- "Samsung, fourth [largest] manufacturer of mobile phones in the world – which account for 10 percent of its sales – has…forbidden the use of [camera phones] in its factories and research departments since July 14th [2003]."[12]

---

[6] Quoted from http://www.detnews.com/2003/technology/0311/30/a01-337955.htm
[7] Quoted from http://www.wired.com/news/infostructure/0,1377,61936,00.html
[8] Taken from http://www.forbes.com/infoimaging/2003/12/10/cx_af_1210camera.html
[9] Taken from http://www.forbes.com/infoimaging/2003/12/10/cx_af_1210camera.html
[10] Taken from http://www.usatoday.com/money/workplace/2004-01-12-phones_x.htm
[11] Taken from http://www.usatoday.com/money/workplace/2004-01-12-phones_x.htm
[12] Quoted from http://www.160characters.org/news.php?action=view&nid=180

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

If even a major camera phone manufacturer (Samsung, above) is forced to ban its own product on company grounds, chances are fairly good that your organization will have to face the reality of this potentially damaging new technology in the very near future, if it hasn't been dealt with already. It is difficult to imagine a company (or an individual, for that matter) who is completely immune to every possible threat posed by camera phones, because this technology by its very nature changes the capacity to take and share pictures on a fundamental level. The proliferation of digital cameras in general has made it more convenient than ever for the average person to snap photos to their heart's content. Whereas in the past many people only bothered to snap photos at special occasions or events due to various inconveniences inherent in photography at that time, digital cameras are smaller and lighter than they used to be, there is no need to carry extra film around, and it is no longer necessary to pay a third party to develop the pictures. However, even with the added conveniences offered by standard digital cameras, people still don't usually carry them around like they would a wallet, purse, or car keys. Camera phones, on the other hand, are built into a device people generally keep near them, which further facilitates their ubiquitous use.[13] This characteristic, along with the relative incognizance on the part of security personnel regarding camera phones and the risks they pose, could potentially create big problems for a company with secrets or sensitive data requiring safekeeping.

THREAT VECTORS

It's probably safe to assume that most organizations usually spend the vast majority of their IT security budgets protecting their existing data from network-based attacks rather than worrying about "malicious digital photography". Sure, there is usually some degree of physical security along with a combination of several other security implementations, but internal and external *network* attacks typically command the lion's share of security practitioners' attention. Digital cameras never really posed an exceptional threat, because many organizations realized that in a situation where a security breach was achieved using a digital camera, all that would be required to fix the problem is to confiscate the camera (and/or the storage media containing the pictures). By taking possession of the camera, they were able to contain the problem and avert the potential distribution of illegally obtained information.

On the contrary, camera phones, with their contentious ability to distribute photographs via the Internet, are much more difficult to contain, if not impossible. Once a captured photograph makes its way out onto the Internet, it becomes fair game for anybody in the world to view, copy, and distribute. You could certainly make every attempt to contain the spread of your confidential information by issuing "cease and desist" letters or by threatening lawsuits, but let's face it- nobody owns the Internet, and clearly no one entity governs it. There could be

[13] Paraphrased from http://64.177.207.251/CIIMA/CIIMA%20V3%20N110%20Dunphy.pdf

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

bits and pieces of your proprietary or confidential data flying around the 'Net unabated for years, and your company's bottom line could sustain a potentially debilitating blow.

Aside from the threat posed by attackers from *outside* your organization, there's plenty of harm that could be inflicted by an organization's own employees:

> "Specifically, camera phones potentially could be used by employees to snoop on other employees and to take photographs of proprietary information and processes" according to Jack Gold, META Group's vice president for Technology Research Services. "Somebody can walk into a bathroom and somebody with a camera phone walks in behind him. It's about sexual harassment, it's about…privacy and, ultimately, it's about protecting intellectual property."[14]

BENEFITS

Considering the sizeable scope of threat vectors involving camera phones, you may be tempted to assume that their potential value to your organization is outweighed by the security risks. Many organizations will ultimately steer clear of camera phones for this reason alone, without even a moment of consideration to the contrary. It might be wise, however, to consider some of the potential benefits of camera phones before drafting excessively stringent security policies in an attempt to prevent them from entering your organization altogether. For instance, in situations where both a camera and a cellular phone are normally required to accomplish a particular task (think insurance adjuster or road surveyor), why not take advantage of a device that already contains both?[15] Let's take a glance at how the potential advantages of camera phones are being realized by several different entities:

- "A real estate agent can email a client photos of a hot property before the property is listed."[16]

- "A construction worker could send a supervisor a photo of say, a crack in a foundation, instead of just describing it, perhaps saving a trip."[17]

- Several months ago a 15-year-old boy narrowly escaped a drive-by kidnapping, then managed to snap a photo of the assailant and his license plate, which ultimately led to the man's arrest. "Even if the guy had been able to grab the camera (or the kid), the photo was [already] out in the ether."[18]

---

[14] Quoted from http://www.internetwk.com/breakingNews/showArticle.jhtml?articleID=16600577
[15] Paraphrased from http://www.richmond.com/business/output.cfm?id=2774814&vertical=business
[16] Quoted from http://www.centredaily.com/mld/centredaily/2003/11/20/news/local/7313357.htm
[17] Quoted from http://www.centredaily.com/mld/centredaily/2003/11/20/news/local/7313357.htm
[18] Paraphrased from http://www.usatoday.com/tech/columnist/andrewkantor/2003-12-11-kantor_x.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- "Emergency [Medical] Technicians use camera phones [from the ambulance en route to the hospital] to photograph injuries to warn…of what's on the way."[19]

- There is a technology in the works which could allow owners of camera phones to scan bar codes on various products in retail establishments and purchase the items electronically- a system which could open up the possibility for countless mobile commerce applications.[20]

ABUSE

It's interesting and somewhat encouraging to think of all the potential innovations camera phones could facilitate, but alas the vast majority of media attention camera phones have garnered in their relatively short history remains predominantly negative. Perhaps under different conditions it would be appropriate to go into greater detail about the many wonderful uses people have discovered for camera phones, but the primary purpose of this paper is to discuss them from a security perspective. For this reason we will stick to discussing the potential ways they can be abused.

As with many promising new technologies which have been developed over the course of history, there will always be uses for those technologies which the creator(s) never intended, and there will always be opportunistic evildoers who are eager to exploit them. Just as quickly as camera phones made their worldwide debut in Japan in October 2002, there were almost immediately reports of some who used the phones for rather nefarious purposes. Ranging from voyeuristic to downright lewd, photographs of unsuspecting people (mostly female) in compromising or revealing positions were being emailed and posted on moblogs worldwide (see the special section on the next page for more info). In addition, a new form of information theft quickly became popular amongst camera phone owners of all ages. Dubbed "digital shoplifting" by industry pundits, thousands of shoppers in a variety of retail establishments were snapping photographs of pages in books and magazines in lieu of purchasing the material.[21] As word spread about the growing number of people and businesses who were being exploited by camera phones, there was increased discussion among government officials regarding possible ways to eliminate the problem.

The South Korean government sought to rectify the situation through the enforcement of new regulations governing the manufacture of camera phones. These new regulations stipulated that beginning in the year 2004 all new camera phones must emit an audible "warning" signal of at least 65 decibels before they snap a picture.[22] Some camera phone manufacturers have chosen to implement

[19] Quoted from http://www.detnews.com/2003/technology/0311/30/a01-337955.htm
[20] Paraphrased from http://www.forbes.com/execpicks/2004/02/17/0217camphonebarcodespinnacor_ii.html
[21] Paraphrased from http://www.silicon.com/networks/mobile/0,39024665,10004931,00.htm
[22] Paraphrased from http://www.courier-journal.com/features/2003/12/20031230camphone.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

this requirement in the form of a recorded voice counting down from five to one prior to the picture being snapped, while others have simply included a quasi-realistic camera shutter sound or a loud beep. Whatever the case, do not assume as a security practitioner that camera phones can be easily identified due to this requirement. There are already several websites with detailed instructions on how to disable the warning signals on a variety of handset models, and these new regulatory requirements do not apply to the millions of camera phones already in consumers' hands.

What exactly is a **"moblog"?**

mobile blog = moblog

Evolved from "blogs" (short for "weblog"). Consist primarily of photographs taken using camera phones which are subsequently posted on a website for others to view. Can include a variety of things: text, picture, audio, or video. Check out the following sites for more info:

www.fotolog.net www.picturephoning.com www.photoblogs.org

www.buzznet.com www.eachday.net

SAFE HAVEN

Given the fact that you cannot easily identify camera phones in real-time as they are brought into your organization, what options do you have available to you as a security practitioner to protect your company from harm? Other than performing a full strip and cavity search on each person entering your facility, there must be an easier (and infinitely less invasive to your employees and visitors) way to stay on top of this threat, wouldn't you assume? If you happen to be looking for a way to control and monitor camera phones electronically, perhaps the best answer to the previous question is "not quite yet." There are currently at least two major companies working on a new technology which temporarily deactivates camera phones' and digital cameras' imaging systems within a localized area.[23] Called "Safe Haven," the technology relies on two key components in order to work properly, according to the company which created it, Iceberg Systems (http://www.icebergsystems.co.uk/index.html). First are the hardware transmitters which are strategically positioned within a building or other structure, and whose job is to intermittently send out infrared signals announcing that a particular area is designated as a "Safe Haven." Once a camera phone or digital camera is brought within the perimeter outlined by the transmitters, they are immediately and silently instructed to disengage their imaging systems.

[23] Paraphrased from http://asia.cnet.com/newstech/communications/0,39001141,39150860,00.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

However, for this signal to be interpreted and enforced there is a second component of the Safe Haven technology which is necessary. This component consists of software which must be installed on the imaging device prior to entering the Safe Haven perimeter. The software typically would have to be installed by the manufacturer of the device, but there is currently a much easier method in the works which will allow users of mobile devices to download the software through their wireless carrier. However, this method relies on end users for compliance, which is clearly less than ideal. Patrick Snow, the managing director of Iceberg Systems, is currently in talks with several major handset manufacturers with his primary goal being to reach an agreement which would make the Safe Haven software a standard component in all new handsets. Until this goal is realized, however, Safe Haven will be of little use to anyone looking to enforce camera phone policies electronically.

One aspect of Safe Haven which may increase the odds of its widespread adoption and use is the fact that there are several other applications of the technology which are not specifically security-related. For instance, Safe Haven can be set up in such a way that all cellular phones within its radius will be unable to ring when an incoming call arrives. It can also be used as a jamming device of sorts, rendering wireless devices temporarily unable to send or receive voice, data, or text. Despite these additional uses, Mr. Snow insists that he is currently only marketing Safe Haven as a security product. [24] Even so, if Safe Haven eventually becomes the camera phone security mechanism of choice by major global handset manufacturers, it remains to be seen how easily existing camera phones could be retrofitted with this technology. Instead of waiting around to see the outcome of this scenario, perhaps a better choice would be to develop or refine an effective security policy now.

RISK ASSESSMENT

With few choices available to provide protection against the threat of camera phones, it may seem a rather daunting task to write security policies to govern them. It should be sufficiently clear by now that your organization is probably in need of a policy to address camera phones directly, but you may be unsure how to begin writing one. Probably a good starting point for most people would be to conduct a brief risk assessment- in other words, exactly how vulnerable is your organization to camera phone misuse? You'll probably want to consider questions such as:

1. Do visitors sometimes have opportunities to take pictures of sensitive material, items, or data they would ordinarily not be able to observe in great detail?

[24] Paraphrased from http://asia.cnet.com/newstech/communications/0,39001141,39150860,00.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

2. Would pictures of your laboratories or specialized equipment be an aid to your competitors, or valuable to someone interested in committing industrial espionage?

3. Are there any critical projects or processes in view of your visitors which, if video of these activities were streamed out to the Internet in near real-time, your company could suffer?

4. How concerned would you be if a visitor to your organization were walking around snapping photos of (key) personnel?

5. Consider what would happen if someone distributed photos they had taken of your company's newest breakthrough and patentable technology early in its development. Would it affect your company's R&D initiatives?[25]

SECURITY POLICY

Once you've had time to conduct a risk assessment, you should begin drawing up the basic framework of your security policy. To ensure that your policy provides for an appropriate measure of strictness, there are a few more key points to consider, such as:

1. Should your policy be one of complete prohibition, or are there locations or facilities within your organization where taking pictures would be acceptable?

2. How will you go about ensuring that everyone is aware of the policy, both employees and visitors if necessary?

3. Who will enforce the policy, and how?

4. Will the policy apply to all cellular phones, or just camera phones?

5. If you've chosen to prohibit the use of camera phones entirely, and you intend to confiscate them at the door, what can you do to identify them to keep each of them separate? How will you keep the phones themselves secure?[26]

With some preparation and planning, you should be able to limit the number of camera phone incidents that occur within your organization. As you previously learned, electronic security mechanisms such as Safe Haven are not

[25] List paraphrased from http://hhi.corecom.com/cameraphonesecurity.html
[26] List paraphrased from http://hhi.corecom.com/cameraphonesecurity.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

yet ready for production (at the time of this writing), so your security policy will have to be relied upon as your main defense in the meantime. However, there is yet another facet of camera phone security to consider. What happens if your security policies and procedures prove ineffective, and some sort of security event involving a camera phone occurs within your organization? What legal recourse do you have?

LEGAL ISSUES

Unfortunately, there is currently no clear-cut answer to that question. The issue is being hotly debated as more and more organizations and individuals fall victim to camera phone misuse. Since camera phones are still a relatively new phenomenon in the United States, there are currently very few, if any, laws written to address their potential for misuse. There have been a few cases which have received a certain degree of media attention, whereas camera phones were expressly forbidden to be brought into courtrooms. However, as for actual laws you'd be extremely hard-pressed to find any that deal specifically with camera phones. This has unfortunately been a recurring theme in our history- laws have almost always been *reactionary* as new technologies forge ahead and bring new challenges. David Sobel, general counsel at the Electronic Privacy Information Center in Washington reinforced this notion when he quipped "Congress hasn't squarely addressed this issue [of camera phone misuse] yet, and it needs to--this is a classic example of technology outpacing the development of the law."[27]

PRIVACY ISSUES

As laws governing camera phones begin to emerge over the next few years, privacy will undoubtedly be a prevalent underlying theme in the vast majority of them. Most people have a fairly deeply-rooted opinion of what the term *privacy* really means, as evidenced by the fact that discussions about privacy will often elicit fierce personal opinions. People generally like to think that privacy is a right, whether the basis of their argument is rooted in legality, constitutionality, religion, or some combination thereof. One would assume that for an issue which seems to affect most people on an almost visceral level that there would be clear legal delineations between which types of privacy are protected constitutionally in the Unites States and those which are not. Without even so much as a universally accepted definition of privacy, however, the establishment of such boundaries proves extremely difficult.

It will be interesting to see how cases involving privacy infringement will pan out in the coming years. There are already perhaps tens of thousands of camera phone owners in the United States who each spend a good portion of their days incessantly snapping photographs of various people with whom they come into contact. Odds are good that eventually some of these unwitting subjects will take offense to having their picture taken, which will in turn raise

[27] Quoted from http://www.csmonitor.com/2003/1107/p13s02-stct.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

some challenging legal questions regarding an individual's legal right to his/her own image. If we examine how this type of scenario has already been dealt with using a different medium, say audio recordings for instance, we may be afforded some insights into the probable outcomes of some of these cases. It is already widely known that in most states "recording conversations without consent is illegal."[28] However, there have been instances where the legality of this issue has been challenged successfully, such as "the U.S. Supreme Court's 2001 decision in Bartnicki v. Vopper, 532 U.S. 514." That particular ruling "held that the First Amendment protected a radio station's use of a recording that resulted from an illegal wiretap."[29] Will improperly procured photos' being distributed on the Internet likewise fall under First Amendment rights?

To say that security cameras and various other forms of surveillance equipment are ubiquitous would obviously be quite an understatement, but what about camera phone "surveillance"? What if a camera phone user has a reasonable and legitimate reason to document his/her surroundings? Do the people who happen to end up in the photos have a legal right to know they have been photographed? "Courts traditionally have held that people do not have an expectation of privacy in public areas, although privacy experts say camera phones may test that idea."[30] This especially rings true when you consider a scenario where someone were to benefit monetarily or otherwise from photography ascertained through camera phone use. For instance, what if a camera-phone wielding fan of a famous celebrity ends up making money from a photograph he/she managed to snap? Should this "pocket paparazzi" be forced to share the earnings? What if a co-worker snaps a picture of you in a compromising or embarrassing situation and subsequently places the photo on a moblog for the world to see? Are you legally entitled to punitive damages if your job status is adversely affected? Issues such as these will doubtless be raised as camera phones begin to ultimately fulfill the astronomical sales predictions, and as more and more surreptitious uses for these devices are conjured up.

CONCLUSION

We live in a world where nearly our every move or decision leaves behind an electronic fingerprint. As the digital landscape continues to evolve, camera phones will undoubtedly play a significant role in shaping a variety of legal, moral, and ethical issues. From a security standpoint, camera phones are clearly a force to be reckoned with, and until technologies such as Safe Haven come to fruition, the range of available security countermeasures will remain fairly narrow and unsophisticated. The best thing you can do for your organization at this point is to ensure that adequate security policies are written and enforced, and that all employees of your organization are well informed of the intricacies therein. It will only be a matter of time until pertinent legislation is passed and public awareness is raised to a point where camera phones are no longer a

[28] Quoted from http://www.nbc4.com/technology/2658781/detail.html
[29] Quoted from http://www.metnews.com/articles/cell101403.htm
[30] Quoted from http://www.usatoday.com/news/nation/2003-10-19-cell-phones_x.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

threat that lurks just beneath the radar. Until then, extreme vigilance will be an absolute requirement in protecting your organization's trade secrets and sensitive information.

REFERENCES

Leggat, Robert. "A History of Photography, by Robert Leggat: DAGUERRE, Louis Jacques Mande" 23 Feb 2004. URL: http://www.rleggat.com/photohistory/history/daguerr.htm

"The Metropolitan Museum of Art - Special Exhibitions: The Dawn of Photography: French Daguerreotypes, 1839–1855." 8 Mar 2002. URL: http://www.metmuseum.org/special/French_Daguerreotypes/dawn_more.htm

"Daguerreotype Photographs: The Daguerreotype." URL: http://memory.loc.gov/ammem/daghtml/dagdag.html

Dunphy, Joseph M. "The Emergence of Camera Phones - Exploratory Study on Ethical and Legal Issues." Communications of the International Information Management Association, Volume 3 Issue. URL: http://64.177.207.251/CIIMA/CIIMA%20V3%20N110%20Dunphy.pdf

Susnjara, Bob. "Picture this — laws covering camera phones laws." *Daily Herald*. 25 Jan 2004. URL: http://www.google.com/search?q=cache:10BUsJLRS-MJ:www.dailyherald.com/search/main_story.asp%3FintID%3D38011297+%22that%27s+more+than+double+the+number+sold+in+2002%22&hl=en&ie=UTF-8

Dybis, Karen. "Businesses shutter camera phones." *The Detroit News.* 30 Nov 2003. URL: http://www.detnews.com/2003/technology/0311/30/a01-337955.htm

Asaravala, Amit. "Camera Phones Help Buyers Beware." *Wired News*. 19 Jan 2004. URL: http://www.wired.com/news/infostructure/0,1377,61936,00.html

Ferrari, Alicia. "Camera Phones Fire A Warning Shot." 10 Dec 2003. URL: http://www.forbes.com/infoimaging/2003/12/10/cx_af_1210camera.html

Armour, Stephanie. "Camera phones don't click at work." *USA Today*. 12 Jan 2004. URL: http://www.usatoday.com/money/workplace/2004-01-12-phones_x.htm

Vassiliou, Marie-Michèle. "First appearance of the phenomenon in South Korea." *160Characters Association.* 10 Oct 2003. URL: http://www.160characters.org/news.php?action=view&nid=180

Haskin, David. "Beware Of Employees Bearing Camera Phones." *InternetWeek.* 9 Dec 2003. URL: http://www.internetwk.com/breakingNews/showArticle.jhtml?articleID=16600577

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Edwards, Donna Johnson. "Talking Tech- All I want for Christmas is my pri-va-cy!" *Richmond.com*. 9 Dec 2003. URL: http://www.richmond.com/business/output.cfm?id=2774814&vertical=business
Nephin, Dan. "Privacy, security concerns prompt camera phone bans." *CentreDaily.com.* 20 Nov 2003. URL: http://www.centredaily.com/mld/centredaily/2003/11/20/news/local/7313357.htm

Kantor, Andrew. "New tech: It's not just the government invading your privacy." *USAToday.* 11 Dec 2003. http://www.usatoday.com/tech/columnist/andrewkantor/2003-12-11-kantor_x.htm

Marek, Sue. "New Technology Enables Camera Phones To Scan Bar Codes." *Forbes.com.* 17 Feb 2004. URL: http://www.forbes.com/execpicks/2004/02/17/0217camphonebarcodespinnacor_ii.html

"Japanese want to stamp out 'digital shoplifting'." *Silicon.com.* 1 Jul 2003. URL: http://www.silicon.com/networks/mobile/0,39024665,10004931,00.htm

Muhammad, Larry. "Smile … you're on candid camphone." *Courier-Journal.com.* 30 Dec 2003. URL: http://www.courier-journal.com/features/2003/12/20031230camphone.html

Kotadia, Munir. "Jamming device aims at camera phones." *CNETAsia.* 12 Sep 2003. URL: http://asia.cnet.com/newstech/communications/0,39001141,39150860,00.htm

Piscitello, David. "Security Policy for... Camera Phones?" 24 Nov 2003. URL: http://hhi.corecom.com/cameraphonesecurity.html

Wolcott, Jennifer. "Cellphone cameras ring warning bells." *The Christian Science Monitor.* 7 Nov 2003. URL: http://www.csmonitor.com/2003/1107/p13s02-stct.htm

Hudson, L.J. "Privacy At Risk: How about privacy in the real world?" *Digital Edge.* URL: http://www.nbc4.com/technology/2658781/detail.html

Watson, David. "Presiding Judge Backtracks on New Camera Cell Phone Policy." *Metropolitan News.* 14 Oct 2003. URL: http://www.metnews.com/articles/cell101403.htm

Jones, Charisse. "Phones make your bad side visible to world." *USAToday.* 19 Oct 2003. URL: http://www.usatoday.com/news/nation/2003-10-19-cell-phones_x.htm

IMAGES & SIDEBARS:

Camera Phone Sales Bar Graph (page 2): www.3g.co.uk/PR/August2003/5738.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Moblog sidebar information (page 7):
http://blog.bitflux.ch/p916.html

© SANS Institute 2004, Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**