# How Safe Are Photo-Sharing Web Sites?

The past few years have seen a sharp rise in the number of digital cameras sold. There has also been a corresponding increase in the number and popularity of publicly hosted Web sites for sharing digital photos. But is it safe to share personal photos on these sites? After all, personal photos contain personal information about you and your family, your interests and hobbies.

A recent spate of violations of privacy stemming from sharing personal information on public Web sites suggests that these sites may not be safe.


Introduction ..... 2
Private Photos on Photo-Sharing Site Sent to the Media ..... 2
Scenario 1: A Web Site Employee May Have Viewed and Copied Photos ..... 3
Scenario 2: Someone May Have "Sniffed" Transmitted Data ..... 3
Scenario 3: Someone May Have Guessed the Couple's Password ..... 4
Scenario 4: The Couple May Have Accidentally Posted Photos in a Public Area of the Web Site ..... 4
Private Photos on Photo-Sharing Site Found by Google ..... 5
Photos on Public Web Site Led to Murder and Kidnapping ..... 5
Personal Information Is Not Safe on Photo-Sharing Sites ..... 6
Recommendations ..... 6
Endnotes ..... 7


SERICON™ technology

February 3, 2005

# Introduction

The past few years has seen a sharp rise in the number of digital cameras sold. There has also been a corresponding increase in the number and popularity of publicly hosted Web sites for sharing digital photos. But is it safe to share personal photos on these sites? After all, personal photos contain personal information about you and your family, your interests and hobbies. Safety in this context means that the personal information, which can be identified and extracted from these photos, is both private and secure.

- *Private* means that access to the information can be restricted to the use of a particular person or group of people. The owner of the information should control who has access to it.

- *Secure* means free from danger and risk of loss, i.e., making sure that the bad guys out there cannot access your information.

A photo-sharing Web site lets members upload and annotate photos that are posted on its site. Some sites offer these services for free, while others charge a fee, sometimes only for additional storage. In general, these sites make money by charging for prints, cards, and gifts such as calendars or coffee mugs imprinted with the photos. Members can share their photos by sending friends and family the URL of their photo site. Sometimes, visitors must enter a username and password in order to view your pictures. Sometimes, this information is embedded in the URL. Often, visitors can leave comments about the photos they view. Some of the better-known photo-sharing Web sites are:

- Webshots (http://www.webshots.com)
- Yahoo! Photos (http://photos.yahoo.com)
- Shutterfly (http://www.shutterfly.com)
- smugmug (http://www.smugmug.com)
- Club Photo (http://www.clubphoto.com)
- dotPhoto (http://www.dotphoto.com)
- Fotopages (http://www.fotopages.com)
- Snapfish (http://www.snapfish.com)

As more people post their pictures online, others are finding ways to exploit them. The Cybercrime Unit of CyberAngels (http://www.cyberangels.org), an organization of IT professionals and law enforcement officers affiliated with the Guardian Angels (http://guardianangels.org), is aware of "a couple of cases of cyberstalking from photo sites."[1] There have already been several documented instances of loss of privacy as a result of pictures and other personal information posted on these Web sites. It is worth examining these cases to understand what went wrong, and exactly where the danger lies.

# Private Photos on Photo-Sharing Site Sent to the Media

The Deseret Morning News, in Salt Lake City, Utah, reported that nude photographs of a prominent married couple were leaked to the press. The couple photographed each other and stored these private pictures at a free online photo-sharing site, believing they would be secure. Somehow, copies of their photos were sent to the news media, which chose not to publish the photos or identify the couple.

The couple insists they never told anyone the photos existed or ever shared them.[2] If we believe them, how could someone else have accessed the photos in order to send them to the media? If we examine several possible scenarios, we can identify possible security breaches.

## Scenario 1: A Web Site Employee May Have Viewed and Copied Photos

An employee of the Web site where the couple's photos were posted may have seen and copied them. In general, even if these sites say they protect your privacy, their employees may be looking at your pictures to make sure they do not violate their terms of service, which are similar. For example, Yahoo!'s terms of service state:

> You agree to not use the Service to… upload, post, email, transmit or otherwise make available any Content that is unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable.[3]

It is reasonable to assume that some Yahoo! employees check content to make sure it complies with the terms of service.[4] However, who is protecting you from these employees? You don't know who they are, or how many employees may have access to your pictures. It is probably safe to assume that someone whom you do not intend will look at the photos you post at any photo-sharing site. In addition, these employees may also be able to access, with or without their employer's consent, other personal information, such as your name, address, and phone number. If you purchased something, such as additional storage space or prints of photos, employees may also be able to access your billing information, such as your credit card number or your bank account information. Employees could use information such as your address and phone number along with identifying information in photos to identify and contact you or your child.

## Scenario 2: Someone May Have "Sniffed" Transmitted Data

Someone may have "sniffed" the data as it traveled between the couple's computer and the computer at the photo-sharing Web site:

There are two ways this could have happened:

- Someone may have "sniffed" the couple's Internet traffic: someone may have targeted them and watched information sent to and from their computer, such as the photos or usernames and passwords, while they were uploaded to the Web site or viewed. It is relatively easy to "sniff" a neighbor's Internet traffic, particularly if you share the same broadband ISP. ISPs have similar terms-of-service agreements. While these agreements generally prohibit watching other customers' traffic, it is easy to do so without being detected.

  For example, Comcast's terms of service indicate the severity of this problem: Its terms include an "acceptable use policy" that prohibits the use or distribution of "tools designed or used for compromising security, such as password guessing programs, decoders, password gatherers, analyzers, cracking tools, packet sniffers, encryption circumvention devices, or Trojan Horse programs." [5]

- Someone may have "sniffed" the Web site's Internet traffic: someone may have watched traffic to the Web site, such as the usernames and passwords when they entered the site, or the photos, while they were uploaded or viewed. Note that an attacker who sniffs data from a Web site has different motives from one who sniffs a target's personal data: in this case, the attacker does not pinpoint a specific individual; instead, the attacker tries to access as much personal information as possible in the hopes of finding something interesting.

**What is packet sniffing?**
When information is transmitted between computers, it is divided up into "packets" that travel separately through the Internet and are reunited at their destination. If you can get between the point of origin and the destination, you can use a packet sniffer to watch the traffic. If the data is unencrypted (i.e. if it does not use SSL), you can see the contents of these packets.

While usernames and passwords may seem secure, they are often transmitted to these sites without secure SSL encryption: they are generally encoded with basic authentication, which is not secure and is easy to decode. (In contrast, usernames and passwords are sent to banking and e-commerce sites securely, using SSL.)

**What is SSL?**
Secure Sockets Layer (SSL) is a commonly used protocol for securely encrypting transmitted data on the Internet.

## Scenario 3: Someone May Have Guessed the Couple's Password

Someone may have guessed the couple's password to the Web site. This could have happened in one of several ways:

- The couple may have used a password that is easy to identify, such as one including a birthday, name, or another easy-to-guess choice.

- The couple may have fallen victim to "social engineering,"[6] which is being tricked into revealing personal information. For example, the couple may have received a telephone call from someone pretending to be a Web site employee who asked for their password. Some people are not sufficiently computer-savvy to realize they should never reveal a password, even to an employee of a legitimate business.

- The couple may have been the victims of a more sophisticated "phishing" scheme, which is fishing for personal information by tricking someone into revealing it. For example, the attacker may actually create an attractive Web site to encourage unsuspecting users to sign in using an e-mail address and a password. It is likely that someone uses the same password to sign into multiple Web sites, and perhaps even to access an e-mail account. By accessing an e-mail account, the attacker can then see e-mail from other Web sites the person belongs to, and can often access those sites, too. Even an attacker who cannot access an e-mail account can try to access other Web sites using your e-mail address or username and password.

## Scenario 4: The Couple May Have Accidentally Posted Photos in a Public Area of the Web Site

The couple may not have understood how the Web site worked, and may have accidentally posted their pictures in a public area rather than in a private, password-protected one.

- For example, at the Yahoo! Photos (http://photos.yahoo.com) photo-sharing Web site, you can mark a photo album as "Private." You can also send out a photo-sharing e-mail invitation, presumably so that visitors can access a public album. It is difficult for someone else to access your pictures on Yahoo! Photos without an invitation, which is a direct link to your album.

  > [Kent] Seamons, [a computer science professor] at BYU noted some instructions at Yahoo! Photos that, if not followed carefully, could allow someone who thinks they are sharing some, but not all, of their photos to easily make everything available.
  > Those instructions say, "If you use Yahoo! Photos to send a photo-sharing invitation, any recipient of that invitation could come view that album even if it is set to Private. Any photo-sharing e-mails you sent through Yahoo! Photos will override the Advanced Sharing Setting for that album."[7]

  Sending an invitation to access photos on a photo-sharing Web site is itself problematic, since e-mail is generally not secure. For example, if you send an e-mail invitation from your home to your friend at work, employees of your ISP can see it, as can the IT professionals at your friend's job. Information sent by e-mail is also susceptible to sniffing attacks, as described above. Anyone who can access the e-mail invitation can, by extension, access your personal photos on a Web site.

- At the Fotopages (http://www.fotopages.com) photo-sharing Web site, you can visit other people's online photo albums (called photo logs). This means that if you post your pictures on this site, any visitor to the site can see your photos . If you want, you can disable this option, but only after you create your online photo albums. So for some time, at least, all posted photos are public, and you must do something specific to mark your photos as private. Visitors can also search other people's pages by country, or even input any term, such as a name or a location into the site's search facility. This makes it easier to find specific information about a person or a place.

## Private Photos on Photo-Sharing Site Found by Google

Sometimes, personal photos become publicly accessible because of a problem with the software at the Web site. For example, after alleged prisoner abuse at the Abu Ghraib prison in Iraq became a top news story, an AP reporter used the Google online search engine to research the prosecution of a group of SEALs who allegedly beat prisoners and photographed one of them in degrading positions.

The reporter found what may be the earliest known photos of the alleged prisoner abuse on the smugmug photo-sharing Web site (http://www.smugmug.com). The woman who posted the photos said they were on the camera her husband had brought back from Iraq after his tour of duty.

"The wife said she was upset that a reporter was able to view the album, which includes family snapshots."[8] The smugmug site states that it is secure: "We give you the option of creating private, password-protected galleries."[9] However, the fact that a search engine found these private pictures on the smugmug site indicates that it was not as secure as it claims. This indicates a software bug or a design flaw in the smugmug Web site.

"'I think it's fair to assume that it would be very hard for most consumers to know all the ways the search engines can discover Web pages,' said smugmug spokesman Chris MacAskill."[10] Certainly, it seems that even the computer professionals at smugmug do not know how to prevent a search engine from discovering people's private information on their own site. Indeed, smugmug violated the trust of its member when a search engine found her personal and supposedly private information.

## Photos on Public Web Site Led to Murder and Kidnapping

In late December 2004, Lisa Montgomery was arrested and charged with kidnapping resulting in the death of Bobbie Joe Stinnett. This was a top news story. Montgomery allegedly met Stinnett at her home, strangled her, cut her fetus out of her womb, and kidnapped the baby. CNN quoted FBI spokesman Jeff Lanza, who said: "Montgomery knew Stinnett was pregnant because of pictures posted on her dog-breeding Web site."[11]

Stinnett's Web site contained personal information: a photograph of herself visibly pregnant. Montgomery allegedly used this information to target Stinnett. Montgomery also gained additional information from Stinnett's Web site, such as the fact that she raised rat terriers. This was sufficient for Montgomery to fabricate a story that she wanted to buy a rat terrier. Montgomery then allegedly contacted Stinnett on the pretext of buying one of her dogs, and gleaned additional personal information, such as her address and when she would be home. Montgomery allegedly arranged a meeting to see the dog, but tragically she killed Stinnett and stole her child instead.

When you post personal information on the Internet, you do so with a specific purpose in mind, such as sharing personal photos with your friends and family, or promoting your business.

However, once personal information is freely available on the Internet, you lose control and knowledge of how it ultimately will be used, and to what end.

The tragedy of Bobbie Jo Stinnett is shocking precisely because she was murdered only for the fetus she was carrying. If Stinnett had not posted a picture of her pregnant self on her Web site, she probably would be alive today and caring for her baby. Seemingly innocuous personal information such as her late stage of pregnancy and her affinity for rat terriers was exploited by her murderer.

So much information is available from personal photos and annotations, as the Fotopages' tagline says, "because a photo is worth a thousand words."[12] Personal photos can powerfully convey a lot of information to those close to you, but when that information is not safeguarded, it may convey this same information to those who would harm you.

## Personal Information Is Not Safe on Photo-Sharing Sites

Both the nude photos of the Utah couple and the SEALs photos became public because private information was in the public domain, where the owners of the information (those who took the pictures) had no control over it. Instead, those who control access to the private information on photo-sharing Web sites are generally corporations in business to make money, not to safeguard your security. If your privacy is violated, you are the one who suffers the loss, not the site. Although usernames and passwords give you feeling of control, this is illusory, since that information is not sent securely, and in any case your personal information can be accessed by Web site employees.

Although Stinnett posted pictures of herself on her own Web site rather than on a photo-sharing site, the effect was the same: personal information was in the public domain, which was exploited by her murderer. Although she controlled her Web site, she did not maintain control of her personal information.

Any publicly accessible Web site is an unsafe place for personal or private information. The Stinnett tragedy shows that identifying details in pictures can be very dangerous. In addition, some photo-sharing sites let you annotate your pictures, and some sites let visitors leave publicly viewable comments. This is very dangerous, because even if you are careful about annotating pictures in a non-identifying way (without names and locations, for examples), visitors to your site who share this knowledge may not be as careful.

Since other people can access your photos on photo-sharing sites, without your consent or knowledge, we can conclude that these sites are neither private nor secure. Therefore, they are not a safe place to store personal information.

## Recommendations

- Avoid putting any personal information on the Internet. However, this is not a satisfactory solution for many people, who already have photos and other media in digital format that they want to share.

- Make CDs containing personal photos and videos and distribute those to friends and family in person or by mail. This is as secure as the method of delivery, but it is expensive, time-consuming, and slow.

- Insist that any photo-sharing site where you post pictures uses secure SSL encryption for transmitting usernames and passwords and data. Currently, no photo-sharing sites have this level of security.

The real solution is to maintain control of your personal information, even when it is on the Internet, just as you maintain control of your other personal property. There are several ways to do this:

- Post personal photos only on a Web site hosted on your computer. This way, you control the information, and the access to it. This also prevents Web site employees from accessing your personal information. There are now several hardware and software solutions that make this easy to do.

- Insist on secure passwords and treat them securely:

    - Use usernames and passwords to control who can access your personal information.

    - Do not distribute usernames and passwords by e-mail, which is not secure. Instead, distribute them by phone.

    - Use SSL when transmitting sensitive information such as usernames and passwords as well as the personal information on your site.

These steps, when taken together, prevent the following problems:

- Sniffing username and password information sent over the Internet to and from your computer, and to and from a Web site.

- Sniffing personal pictures sent over the Internet to and from your computer, and to and from a Web site.

---

Founded in 2004, Sericon Technology is an independent software vendor committed to making the Internet more useful and easier to use for both corporate and consumer users.

Its patent-pending technology enables photo-sharing software to transmit personal information securely.

For more information, visit http://www.sericontech.com.

# Endnotes

[1] Personal e-mail correspondence with the author of this article, January 2005.
[2] Davidson, Lee and Dillon Kinkead, Lucinda, "'Raid' can be embarrassing – or worse," Deseret Morning News, Salt Lake City, Utah, January 2, 2005 (http://deseretnews.com/dn/view/0,1249,600101955,00.html)
[3] Yahoo! Terms of Service (http://docs.yahoo.com/info/terms)
[4] Joseph Touch at the University of Southern California Information Sciences Institute wonders: "They — might — be checking what is posted to ensure these terms are followed," he said, noting that at least company officials could be looking at photos there to police for objectionable items." In Davidson, Lee and Dillon Kinkead, Lucinda, "'Raid' can be embarrassing – or worse," Deseret Morning News, Salt Lake City, Utah, January 2, 2005 (http://deseretnews.com/dn/view/0,1249,600101955,00.html)
[5] Comcast Terms of Service, Comcast High-Speed Internet Acceptable Use Policy (http://www.comcast.net/terms/use.jsp)
[6] Many social engineering attacks are described in the book, "The Art of Deception: Controlling the Human Element of Security," by Kevin D. Mitnick, published by Wiley, 2002.
[7] Davidson, Lee and Dillon Kinkead, Lucinda, "'Raid' can be embarrassing – or worse," Deseret Morning News, Salt Lake City, Utah, January 2, 2005 (http://deseretnews.com/dn/view/0,1249,600101955,00.html)
[8] Hettena, Seth, "AP: Navy Probes New Iraq Prisoner Photos," myway, Dec 3, 2004, 9:04 PM (ET) (http://apnews.myway.com/article/20041204/D86OHMJ80.html)
[9] smugmug privacy policy (http://www.smugmug.com/aboutus/privacy.mg)

[10] Hettena, Seth, “AP: Navy Probes New Iraq Prisoner Photos,” myway, Dec 3, 2004, 9:04 PM (ET) (http://apnews.myway.com/article/20041204/D86OHMJ80.html)
[11] “Couple allegedly showed off kidnapped baby,“ CNN, Monday, December 20, 2004 Posted: 1506 GMT (http://edition.cnn.com/2004/LAW/12/19/missouri.fetus/index.html)
[12] Fotopages (http://www.fotopages.com)