Photo Sharing - Do's and Don'ts

- Only share photos with people you know and trust. Assume that ANYONE can see, copy, and forward photos you post and share.
- Ensure that your family takes similar precautions with their photos; their privacy and sharing settings can expose your images.
- Avoid posting or tagging images that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed.
- Do not use your face as a profile photo, and do NOT enable Location Services for your smartphone camera or photo sharing app.

Choosing the Right Photo Sharing Service

Choosing the right photo sharing service for your needs depends both on your intent and your audience. Key questions to ask are:

- Are you sharing photos primarily for yourself, your friends and family, or for public use?
- Are your contacts or viewers already using a specific service?
- How much control do you need to maintain over your images? Is the retention of EXIF data problematic?

Your choice of photo sharing service determines the amount of control you retain over your images. All services allow you to remove images, but not all services allow for account deletion. However, deleting your content or your account does not ensure removal from the internet.

Nine popular photo sharing services are described below. Default settings are in bold.

<table>
<thead>
<tr>
<th>Service</th>
<th>Primary Use</th>
<th>Image Privacy Options</th>
<th>Displays EXIF?</th>
<th>Location Adding Options (non-EXIF)</th>
<th>Allows Reposting?</th>
<th>Google Indexed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flickr</td>
<td>Share photos within grouped user environments</td>
<td>Public, Private, Contacts, Family, Friends</td>
<td>Yes, No</td>
<td>Editable location, map based</td>
<td>Yes, No</td>
<td>If Public (can opt-out)</td>
</tr>
<tr>
<td>Facebook</td>
<td>Social Network</td>
<td>Public, Only Me, Friends, Friends of Friends</td>
<td>No</td>
<td>Free-form text, linked to Facebook page, map based</td>
<td>Yes</td>
<td>If Public</td>
</tr>
<tr>
<td>Instagram</td>
<td>Share photos from camera enabled mobile devices</td>
<td>Public, Requests to follow must be approved</td>
<td>No</td>
<td>GPS-based device location; Customizable location, text search</td>
<td>No</td>
<td>If third-party apps enabled</td>
</tr>
<tr>
<td>Photobucket</td>
<td>Share photos publicly or privately</td>
<td>Public, Private (optional password protection)</td>
<td>Yes, No</td>
<td>None</td>
<td>Yes</td>
<td>If Public</td>
</tr>
<tr>
<td>G+</td>
<td>Social Network</td>
<td>Circles, Only You, Public</td>
<td>Yes</td>
<td>Editable location, map based</td>
<td>Yes</td>
<td>If Public</td>
</tr>
<tr>
<td>Twitter</td>
<td>Social Network</td>
<td>Public, Requests to follow must be approved</td>
<td>No</td>
<td>Non-editable GPS location for mobile; Text selection for website (city, state)</td>
<td>Yes</td>
<td>If Public</td>
</tr>
<tr>
<td>Yfrog</td>
<td>Enhanced photo sharing in Twitter</td>
<td>None, based on Twitter</td>
<td>No</td>
<td>None</td>
<td>Yes</td>
<td>If Public</td>
</tr>
<tr>
<td>Pinterest</td>
<td>Share concepts and ideas using images</td>
<td>Public</td>
<td>Yes</td>
<td>None</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flickr - Allows detailed control over phone sharing

In upper right, go to Camera > Settings > Privacy & Permissions. Set as follows:

- Who can access your original image files? Your friends and family or Only you
- Allow others to share your stuff? No
- Who can add you to a photo? Only You, edit > Remove me from all photos
- Who can print your photos? Only you
- Allow your stuff to be added to a gallery? No
- Hide your EXIF data? Yes
- Show which application you used for uploading? No
- Hide your stuff from public searches? Check all three
- Who can see what’s on your profile? Friends and family
- Who will be able to see, comment on...? Friends and family
- Who will be able to see your stuff on a map? Only you
- Import EXIF location data? No

Facebook - Compresses images & deletes EXIF, increasing privacy

Go to Triangle > Settings > Privacy.

- Who can see your future posts? Friends
- Limit the audience for old posts...? Limit Old Posts

Then click timeline and tagging. Set as follows:

- Who can post on your timeline? Friends
- Review posts friends tag you in before they appear on your timeline? Enabled
- Who can see posts you’ve been tagged in on your timeline? Friends
- Who can see what others post on your timeline? Friends
- Review tags people add to your own posts on Facebook? On
- When you are tagged in a post, who do you want to add to the audience if they aren’t already in it? Only Me
- Who sees tag suggestions when photos that look like you are uploaded? No One
Photo Sharing Services Smart Card

Instagram - Photos public by default, can be made private
Follow these pictographic instructions for Instagram on the iPhone:

Google+ - Retains all EXIF, multiple privacy settings
Navigate to Google+ Dropdown Menu > Settings.
Under Photos and Videos, set as follows:

- Show geolocation information... Uncheck
- Allow viewers to download my photos and videos. Uncheck
- Find my face in photos and videos... Uncheck
- People whose tags of you are automatically approved... Groups and persons

Under Profile, set as follows:

- Show these profile tabs to visitors... Uncheck all

Under Hashtags, set as follows:

- Add related hashtag from Google... Uncheck

Under Location settings, set as follows:

- Enable location sharing... Uncheck

Yfrog Services - Removes EXIF, privacy settings very limited
Yfrog can be used to post links to photos on Twitter and has also become its own social network called Yfrog Social. When using Yfrog with Twitter, go to Settings and disable photo tagging.

When using Yfrog Social navigate Settings > Account Info and set the profile to private. Individual privacy settings can also be chosen for each picture and album during upload.

Usable Links - For more information or questions regarding this card email smartcards@novetta.com

U.S. Army Social Media Roundup
Washington State Web Wise
Microsoft Safety & Security
OnGuard Online

http://www.atg.wa.gov/InternetSafety/SharingOnline.aspx
http://www.microsoft.com/security/online-privacy/location-services.aspx
http://www.onguardonline.gov/articles/0033-heads