



Photo Sharing Services Smart Card

PhotoSharingServices 060513_1406

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 consumption?
- 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.

| Service | Primary Use | Image Privacy Options | Keeps EXIF? | Location Adding Options (non-EXIF) | Allows Reposting? | Google Indexed? |
|---|---|--|-----------------|--|-------------------|-------------------------|
|  | Share photos within grouped user environments | Private, Contacts, Family, Friends, Public | Yes , No | Editable location, map based | Yes , No | If Public (can opt-out) |
|  | Social Network | Only Me, Friends, Friends of Friends, Public | No | Free-form text, linked to Facebook page, map based | Yes | If Public |
|  | Share photos from camera enabled mobile devices | Requests to follow must be approved, Public | No | GPS-based device location; Customizable location, text search | No | No |
|  | Share photos publicly or privately | Public , Private (optional password protection) | Yes , No | None | Yes | If Public |
|  | Social Network | Only you, Circles , Public | Yes | Editable location, map based | Yes | If Public |
|  | RSS Feed | Requests to follow must be approved, Public | No | Non-editable GPS location for mobile; Text selection for website (city, state) | Yes | If Public |
|  | Enhanced photo sharing in Twitter | None , based on Twitter | Yes , No | Website-based location, or GPS-based for smartphone | Yes | If Public |
|  | Enhanced photo sharing in Twitter | None , based on Twitter | No | None | Yes | If Public |
|  | Share concepts and ideas using images | Public | Yes | None | Yes | Yes |

Instructions for restricting visibility, searchability, and location data retention for each photo sharing service are provided below.

Flickr – Allows detailed control over photo sharing

In the upper left of the page go to *You >> Your Account >> Privacy & Permissions*. Set as follows:

- Allow others to share your stuff? *No*
- Who can add you to a photo? *Only You, edit >> Remove me from all photos*
- 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? *edit >> Yes to all three*
- Who will be able to see, comment on, add notes, or add people? *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 *Privacy Settings*.

- Set Who can see your future posts = *Friends*
 - Limit the audience for old posts on your timeline
- 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? *On*
 - 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*

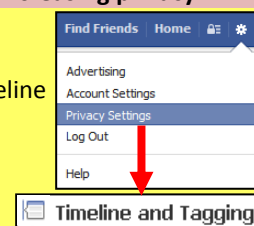


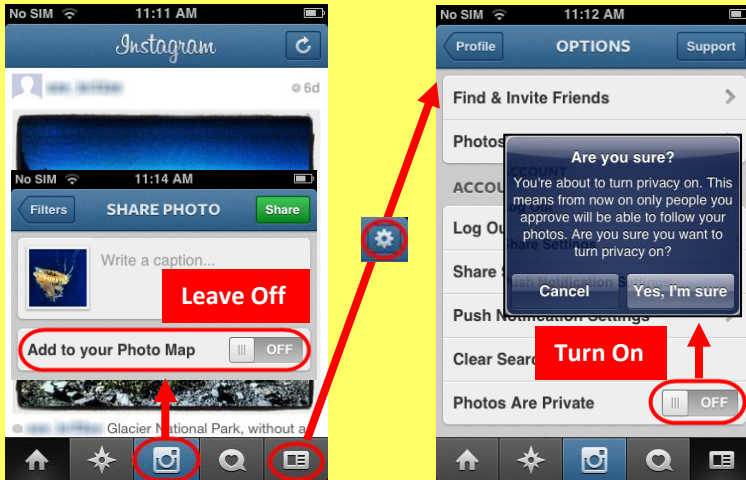


Photo Sharing Services Smart Card

PhotoSharingServices 060513_1406

Instagram – Closed network,

Follow these pictographic instructions for Instagram on the iPhone:



Photobucket – Allows for password--protected sharing

In the upper right go to *User Settings*. On the *Albums* tab, uncheck all options listed under *Links* except *Link back to albums*.

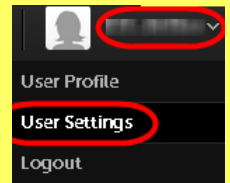
On the *Privacy* tab set as follows:

- Check: *Allow comments in my albums*
- Uncheck: *Show where my photos were taken*
- Uncheck: *Allow others to copy my photos & videos*
- Check: *When I upload, permanently remove information about where my photos were taken*
- Check: *Allow others to follow me*

Under *Privacy* tab > *Album Privacy*, for each album choose to either:

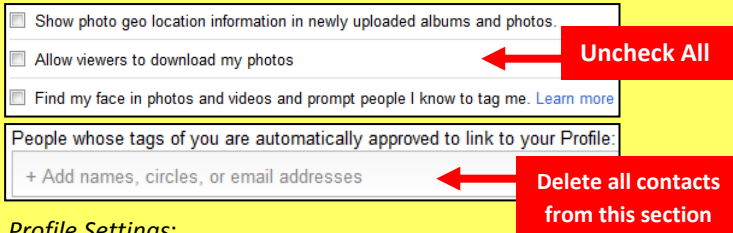
- *Make Private* – Only you can view, or
- *Password Protect* – Anyone with the URL link and the password can view

Remember, choose unique passwords for each album

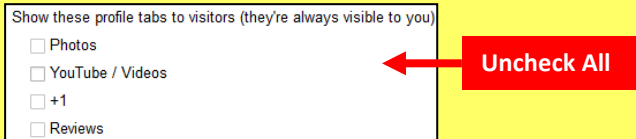


Google+ – Retains all EXIF, multiple privacy settings

Navigate *Settings* >> *Google+* and apply the following Settings.
Photo Settings:



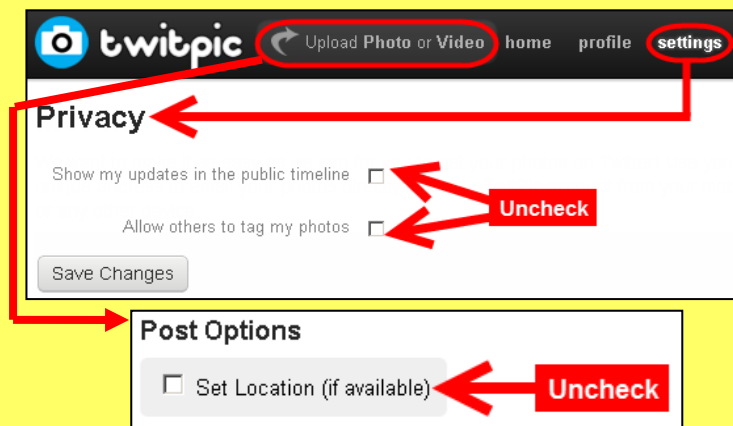
Profile Settings:



Location Settings: disable location sharing and set to *Only You*

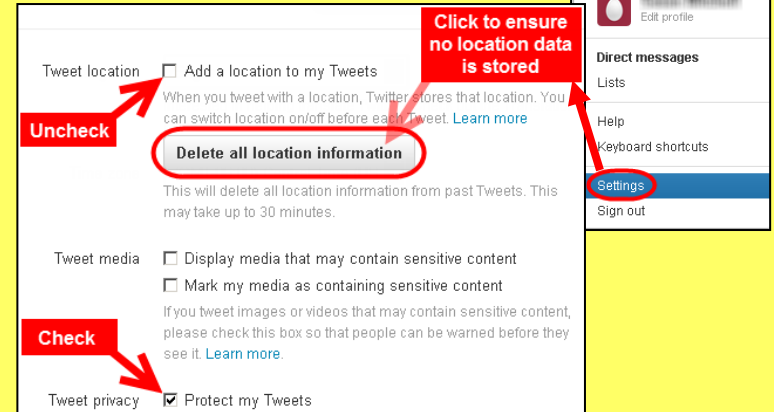
Twitpic – Retains EXIF, privacy settings limited

Twitpic posts links to photos on Twitter. Twitter's privacy settings should be used in conjunction with the native security settings below. Follow these browser-based pictographic instructions for Twitpic:



Twitter – Removes EXIF, but minimal options to limit visibility

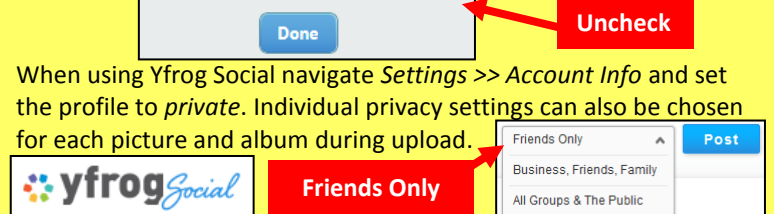
In the upper right go to *Settings*. Once on the *Settings* page, set indicated options as shown.



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.

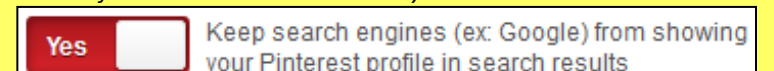
When using Yfrog with Twitter, go to *Settings* and disable photo tagging.



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.

Pinterest – Retains EXIF, privacy settings very limited

In the upper right go to *Settings* under the drop down menu. Under *Basic Information* turn *Search Privacy On*.



Useful Links

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

<http://dmna.ny.gov/members/geotagging.pdf>
<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>

