6 Social Media Considerations for Deployed Soldiers and Their Families

Agenda

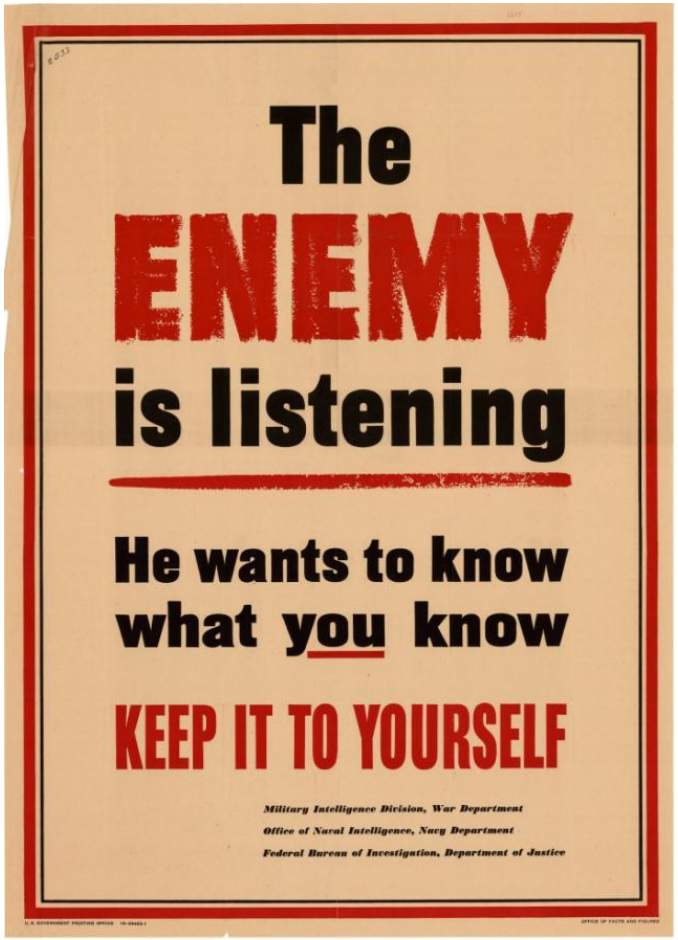
- Introduction
- #1 Social media/online conduct
- #2 Who you connect with
- #3 Privacy settings
- #4 Geotagging safety
- #5 Educating your family
- #6 What not to post
- Resources

Introduction

- Social media has become a big part of our lives. Social media can help people and Army organizations share information during deployments. Social media also helps Soldiers, family members and Army civilians stay connected to loved ones.
- As a culture, we depend on social media, but social media use can be extremely dangerous if you’re not careful, especially when deployed.
- Operations security (OPSEC) and personal privacy concerns should be paramount when using social media whether you’re deployed, or you’re simply staying in touch with your deployed Soldier.

#1 Social media/online conduct

- Soldiers are personally responsible for all content they publish on social media sites, blogs, or other websites.
- Soldiers must be thoughtful about mission-related and non-Soldier related content they post. The lines between a Soldier's personal and professional life often blur in the online space.
- A Soldier who violates Federal law, regulations or policies through inappropriate personal online activity is subject to disciplinary action under the Uniform Code of Military Justice (UCMJ).
- The Army is always working to protect itself against security breaches. It is vitally important that Army leaders, Soldiers and Army civilians understand what kind of data they are broadcasting and what they can do to protect themselves and their families.

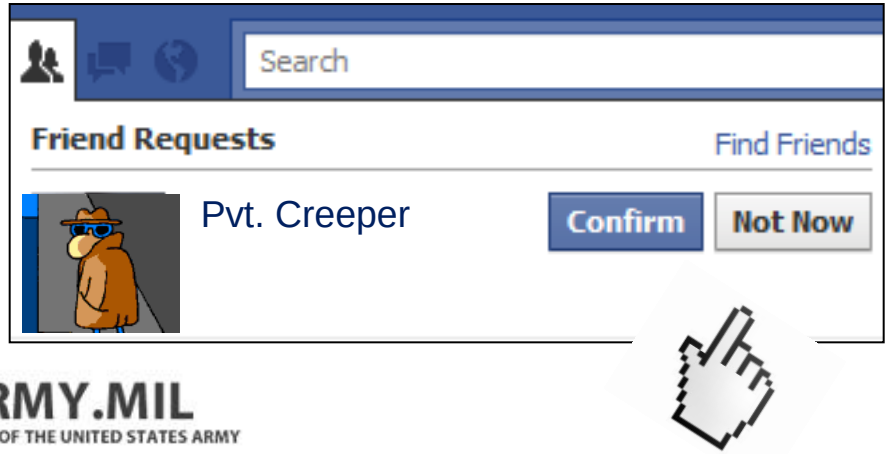


#1 Social media/online conduct

- The posting or disclosure of internal Army documents or information that the Army has not officially released to the public is prohibited. This policy applies no matter how a Soldier comes into possession of a document, video or photo.
- A few examples of unreleased information Soldiers are prohibited from posting include information about causalities, detainees or military operations.

#2 Who you connect with

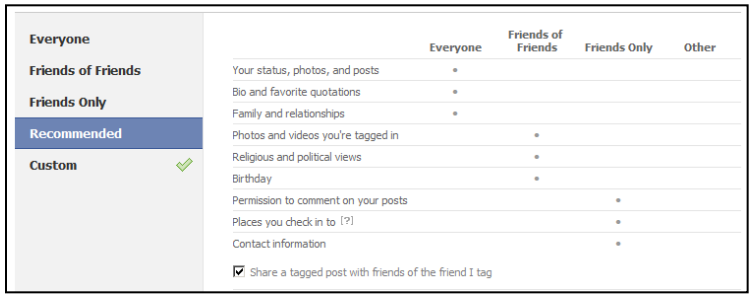
- Be cautious when accepting friend requests and interacting with people online. You should never accept a friend request from someone you do not know, even if they know a friend of yours. For more on this, check out this article about the Robin Sage Experiment: “Fictitious femme fatale fooled cybersecurity” http://goo.gl/Ocf7e
- Don’t share information that you don’t want to become public. Be careful about what you post about yourself on social media platforms. Once you put something out there, you can’t control where it goes. Someone might target you based simply because you work in the Department of Defense. Be cautious when listing your job, military organization, education and contact information.
- Providing too much information in your profile can leave you exposed to people who want to steal your identity or steal sensitive operational information.

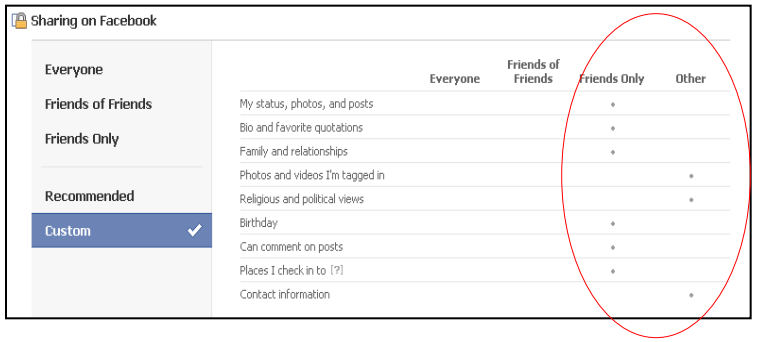


#3 Privacy settings

- Understanding what you can and cannot post on social media platforms goes a long way in protecting yourself online, but more can be done by adjusting your privacy settings on social media sites.
- Facebook's default privacy settings are often public, but Facebook provides various setting options that help Facebook users adjust privacy settings.
- Twitter allows users to keep their Tweets private and Flickr gives users the option of keeping photos private. The settings are easily accessible, the trick is setting them to meet your privacy needs. Similar privacy settings can be found on other social media sites like Myspace and LinkedIn.

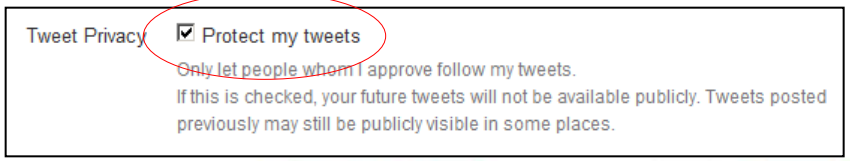
Facebook





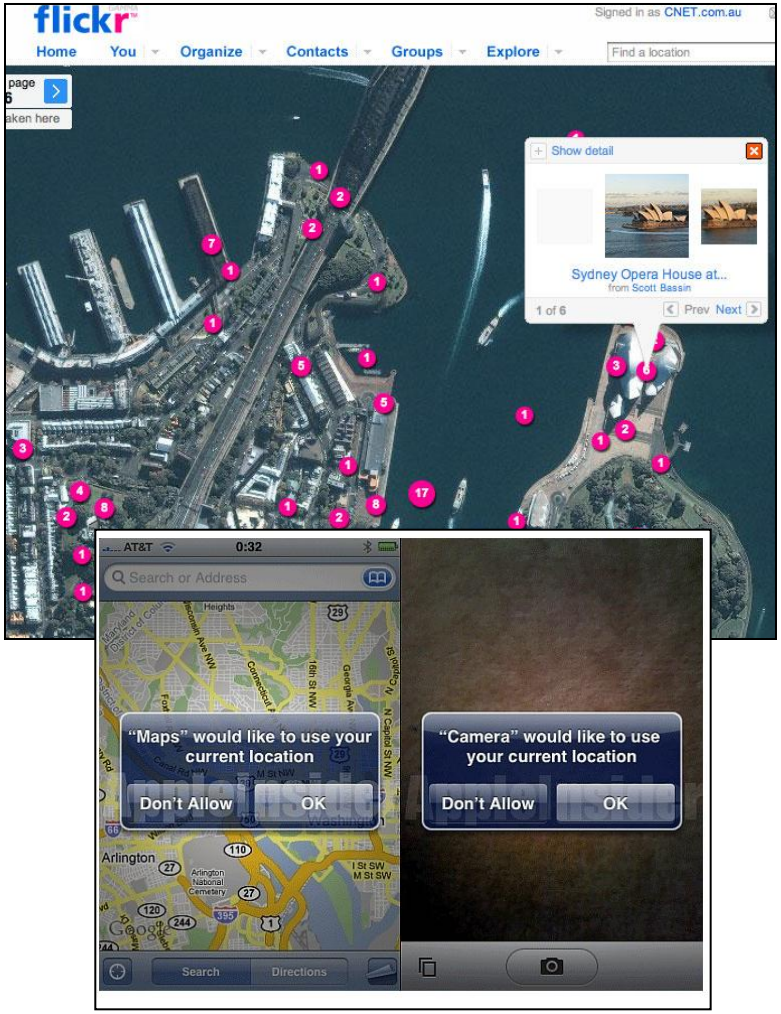
On the top are Facebook's sharing recommendations, below that are the Army's sharing recommendations. For more information about protecting yourself on Facebook, check out this Social Media Roundup: http://goo.gl/2WAlu

Twitter



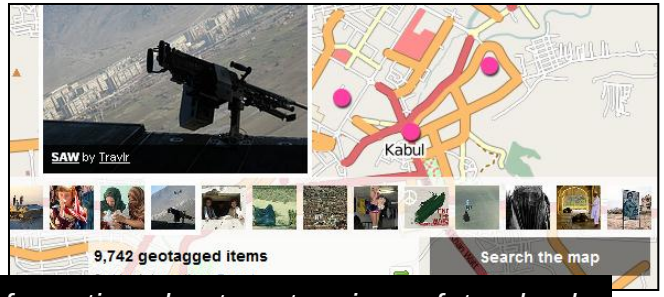
#4 Geotagging safety

- Geotagging is the process of adding geographical identification to photographs, video, websites and SMS messages. It is the equivalent of adding a 10-digit grid coordinate to everything you post on the internet.
- Geotags are automatically embedded in some pictures taken with smartphones. Many people are unaware of the fact that the photos they take with their smartphones and load to the Internet have been geotagged.
- Photos posted to photo sharing sites like Flickr and Picasa can also be tagged with location, but it is not an automatic function.
- For more information about geotagging, check out this website: http://goo.gl/DmJoq

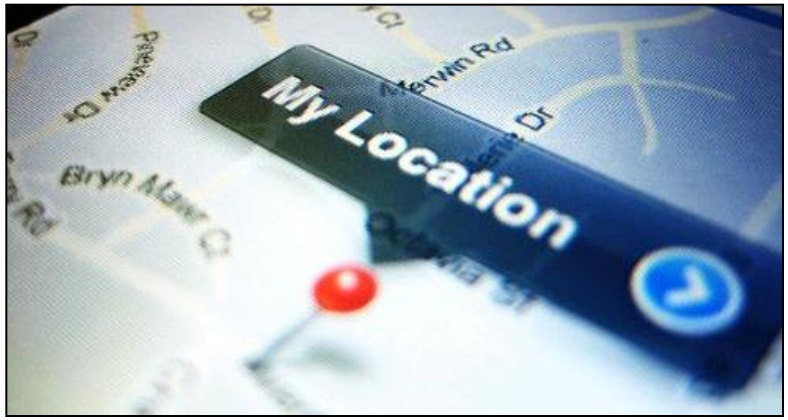


#4 Geotagging safety

- Location-based social networking is quickly growing in popularity. A variety of applications are capitalizing on users' desire to broadcast their geographic location.
- The increased popularity of these applications is changing the way we as a digital culture view security and privacy on an individual level. These changes in perception are also creating OPSEC concerns on an Army level.
- Deployed Soldiers, or Soldiers conducting operations in classified areas should not use location-based social networking services. These services will bring the enemy right to the Army's doorstep.
- Want to avoid giving away location? Disable the GPS function on your smartphone. For instructions on how to do that, check out this website: http://goo.gl/IAmsY



For more information about geotagging safety, check out this Social Media Roundup: http://goo.gl/dyIjB



#5 Educating your family

- Social media helps Family Readiness Groups and Army family members stay connected, but OPSEC should always be the primary concern.
- Family Readiness Groups, Army spouses and Army Family members need to know that posting sensitive information can be detrimental to Soldier safety.
- Ensure that information posted online has no significant value to the enemy. Always assume that the enemy is reading every post made to a social media platform.
- Even seemingly innocent posts about a family member's deployment or redeployment date can put them at risk.

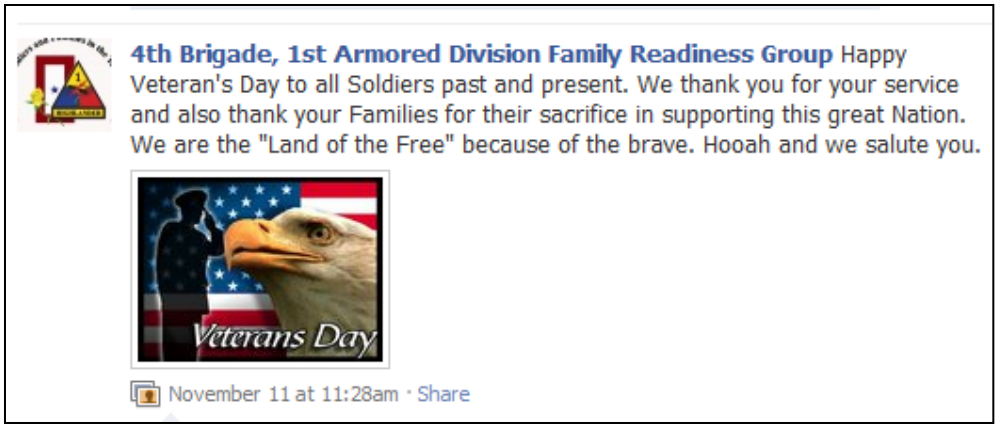
Security items to consider

- Take a close look at all privacy settings. Set security options to allow visibility to "friends only."
- Do not reveal sensitive information about yourself such as schedules and event locations.
- Ask, "What could the wrong person do with this information?" and "Could it compromise the safety of myself, my family or my unit?"
- Geotagging is a feature that reveals your location to other people within your network. Consider turning off the GPS function of your smartphone.
- Closely review photos before they go online. Make sure they do not give away sensitive information which could be dangerous if released.
- Make sure to talk to family about operations security and what can and cannot be posted.
- Videos can go viral quickly, make sure they don't give away sensitive information.

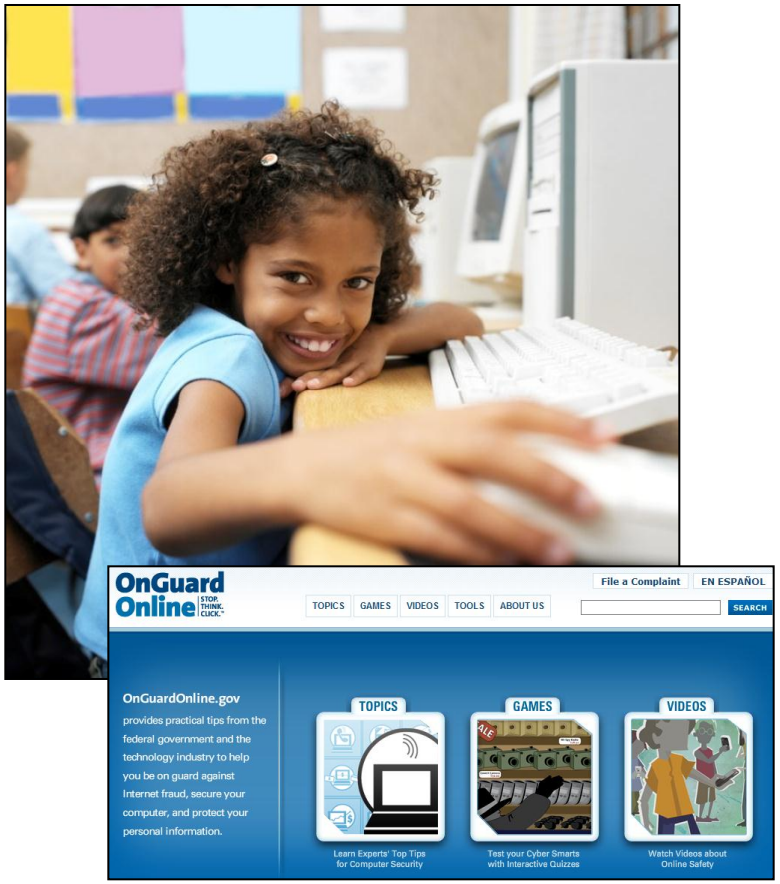
#5 Educating your family

Items authorized to discuss on social media platforms

- Pride and support for service, units, specialties, and service member
- Generalizations about service or duty
- General status of the location of a unit ("operating in southern Afghanistan" as opposed to "operating in the village of Hajano Kali in Arghandab district in southern Afghanistan")
- Any other information already in the public domain posted by official sources



#5 Educating your family



- What is the best way to protect your kids online? Talk to them. Research suggests that when children want important information, most rely on their parents.
- The important thing is to start the education early. Talk to your children about online risks and make sure you create an honest and open environment.
- Some social media sites like Facebook, provide family safety resources and tools for reporting issues: http://goo.gl/sLBym
- Make sure you check out www.Onguardonline.com to find more resources that will help protect your family and yourself online.

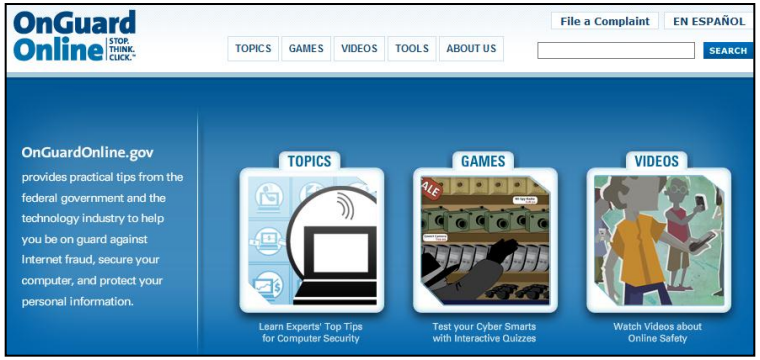
#6 What not to post

- When using Facebook and other social media platforms, do not post personally identifiable information and any information that can damage Army operations.
- Think about what you're posting before hitting share. Many times, you can avoid releasing sensitive information by simply rephrasing your social media post.
- If you aren't comfortable placing the same information on a sign in your front yard, don't put it online.

MAKING DANGEROUS SOCIAL MEDIA POSTS SAFER	
Dangerous	Safer
My Soldier is in XYZ at ABC Camp in ABC City, Afghanistan.	My Soldier is deployed to Afghanistan.
My Soldier will be leaving Kuwait and heading to Iraq in three days.	My Soldier deployed this week.
My Soldier is coming back at XYZ time on XYZ day.	My Soldier will be home this summer.
My family is back in Edwardsville, IL.	I'm from the Midwest.

OPSEC resources

- OPSEC resources
  - Interagency OPSEC Support Staff: www.ioss.gov
  - Anti-Phishing Phil: http://goo.gl/ZFkY3
  - OnGuard Online: www.onguardonline.gov
- Social media training: http://goo.gl/AqmE1
- Social Media Roundups
  - 9 Critical Steps to Protecting Yourself on Facebook: http://goo.gl/igGzN
  - Geotags and Location-based Social Networking: http://goo.gl/wqKwZ
  - Social Media For Family Readiness Groups: http://goo.gl/rS88l
- Army Slideshare site: http://www.slideshare.net/usarmysocialmedia



Contact information

U.S. Army Online and Social Media Division
Ocpa.osmd@us.army.mil

Brittany Brown
U.S. Army Social Media Manager
Brittany.A.Brown@us.army.mil
703.614.4314