New Age Soldier and Social Media: Consequences and Recommendations

TS BAINS

Social media/platforms have started becoming an integral part of our lives, yet they pose dangers/risks for uniformed personnel and their families. Social media provides an easy medium for our adversaries to identify, monitor, target and gain information of value which is detrimental to our nation's security. We are sometimes either unaware of the threats or deliberately choose to ignore them. Adversaries find our family members easy victims to extract information without them knowing it. Peer pressure and societal changes at times force us to be active on social media platforms; however, the need to be careful and vigilant is paramount in the present circumstances. It is possible to safely navigate the social media if we take a few simple measures to mitigate the risks.

The Army Cyber Security Policy 2012 lays down the policy on Social Networking and is reproduced for information

> Social networking sites like Facebook, Twitter, Orkut, groups, technical forums, security forums, education and research forums, blog sites, photo sharing sites can be used **for personal use only** to communicate with family members and friends. However, the same will not be accessed using official communication devices and in office premises. The user will neither create nor join any community, group, etc that is related to terrorism, anti-national elements, political groups, etc. Creation or joining of communities/groups/ email-IDs revealing course, batch, unit, etc revealing any affiliation with

Army, for e.g. NDA 53, YO 120, tiger36sikh@rediffmail.com, awwalrisala@gmail.com, wecandoit.com, etc is prohibited. Any online participation, polling, campaign, etc related to Armed Forces or Govt of India, online interaction with media houses, foreign nationals and agencies/organisations, retired service personnel over official matters is also restricted. No individual will reveal personal identity by way of ranks, appointments, official address or photographs in uniform on the internet.'

Social media platforms are an easy medium to gain information.

The most used social platforms by the armed forces personnel and their families today are Facebook and WhatsApp, with other platforms like Twitter, Hike, Viber, Instagram, Tumblr, etc also gaining ground. We are duty bound to use these within the laid down cyber policy. Therefore, the questions which beg answers are: What are the risks facing us? Are we aware of the risks? What should we do to avoid these so that we can have a better social networking experience?

The cyber security policy is laid down primarily to ensure security of information of the armed forces as also to ensure that we do not fall prey to inimical elements due to our acts of omission or commission. This article looks specifically at risks pertaining to Facebook and WhatsApp within the ambit of the policy, with tips on using your smartphones smartly.

Facebook

It is one of the most actively used social networking sites. Our identity footprint should be kept to the minimum to avoid potential loss of data. A clear understanding of basic issues like Profile Settings, Posting of Pictures, Comments, Tagging and Changes to Facebook Data Policy will enable the user to steer clear of any inadvertent slip-ups. Every user must focus on the under-mentioned tips while carrying out the Profile Settings.

Name: Do not disclose your full name. Use nicknames or jumbled names or reversed names. Keep the 'who can look you up' settings to friends only or friends of friends.

Photo: Put up a scenery photo or a group photo which makes it difficult to identify you individually.

Location: Do not update your current city to your current posting location. You should at best give your home station. Also, do not give location when uploading photos. Note that Facebook tracks location data to enable it to show advertisements on your newsfeed.

Identity footprints on social media has to be minimum to avoid loss of information.

Tagging: Either totally avoid tagging or keep it to the minimum. Sometimes our friends inadvertently give out information by tagging a name in a photo which we would not have posted online. The best option is to make photographs visible to yourself. Else, the user can change the settings by going to Timeline and Tagging to set review tags and make it visible to him only. If you find yourself tagged in a photo, you can go to that photo and untag yourself. You should also limit tagging of your friends as a courtesy so that their photos don't become public without their knowledge. Another common mistake is naming the photo album as xx Course Get-together.

Segregating Friends: One brute method is to have separate Facebook accounts to ensure that your close group remains in one account and others on an account where you only share few things. Facebook has the facility to make groups in which case you will have to ensure that you post only in the groups you want to post and not on your timeline.

Other Information: Do not give the year in your birth date details. Do not give school details/college details, especially of Jawaharlal Nehru University (JNU). Information of value can be deduced from such basic data.

The user can check the correctness of settings by going to Your Profile and then check 'View as' tab next to view activity log.

Comments: This is another potential source of information leakage. One has to be extremely careful while expressing views or sending messages which seem to be above board but can provide valuable data to the analyst. A few examples of comments routinely seen on Facebook are:

> Yipee – moving to Mhow for HC.
> Congratulations to xxx batch on empanelment in 2 SB. List of offrs empanelled is xxx,yyy,zzz.
> Congrats on taking over abc brigade. Best of luck

Changes to Facebook Data Policy: Facebook has recently changed its Data Policy which has been effective since January 30, 2015, and is available at https://www.facebook.com/about/privacy/update. Every user must read it to understand how personal data/information is used. To limit your data access, you need to limit access by changing your privacy settings. The privacy basics can be accessed at https://www.facebook.com/about/basics. Though it will take some time for you to go through it, the tutorial is well explained through images

and actions and is well worth spending time on. It will ensure that you and your family can safely use Facebook.

Essential Checklist for Every User

- Go to general tab of https://www.facebook.com/settings and download a copy of Facebook data. Peruse through it to check if you have inadvertently posted information/pictures you should have avoided.
- Go to https://www.facebook.com/about/basics/what-others-see-about-you/ to learn about who all see your posts. Always choose the option of friends or close friends. Uncheck the friends of tagged option in custom privacy. Avoid using the public option. You can create new lists or restricted lists and post as per the audience you want the post to see.
- If you don't like a post, you can delete it or hide it from your timeline. Never hide it from your timeline as that post can still be accessed. It is better to edit a post rather than deleting it(reason explained a little later).
- You also have a responsibility that no one should get details of other friends/officers accounts through your Facebook account. Go to own profile>friends>edit privacy to select 'only me' option.
- Most social networks allow you to integrate information with other social networks. For example, you can post an update on your Twitter account and have it automatically posted on your Facebook account as well. Be particularly **careful when integrating your social network accounts!** You may be anonymous on one site, but exposed when using another.

WhatsApp

WhatsApp is a popular app being used on mobile phones. The idea of just signing up from a phone number, easy interface, conversation style messaging and optimised CPU are the reasons for WhatsApp's phenomenal success. The service is free for one year and after that it asks you to pay a nominal yearly amount. So, is WhatsApp good, bad or ugly?

Let us first look at an extract of the WhatsApp Terms of Service.

- You hereby give your express consent to WhatsApp to *access your contact list and/or address book* for mobile phone numbers in order to provide and use the service.
- Currently, we have no method of providing different levels of visibility of your status submissions among users that have your mobile phone number – *you acknowledge and agree that any status submissions may be globally viewed* by users that have your mobile phone number, so don't

submit or post status messages or profile photos that you don't want to be seen globally.

- In order to provide the WhatsApp service, WhatsApp will periodically access your address book or contact list on your mobile phone to locate the mobile phone numbers of other WhatsApp users ("in-network" numbers). WhatsApp uses both session cookies and persistent cookies. A persistent cookie remains after you close your browser.
- When you use the WhatsApp site, our servers automatically record certain information that your web browser sends whenever you visit any website. These server logs may include information such as your web request, Internet Protocol ("IP") address, browser type, browser language, referring / exit pages and URLs, platform type, number of clicks, domain names, landing pages, pages viewed and the order of those pages, the amount of time spent on particular pages, the date and time of your request, one or more cookies that may uniquely identify your browser, your phone number, phone number you are requesting the status of and various status information.
- *We may share your personally identifiable Information with third party service providers* to the extent that it is reasonably necessary to perform, improve or maintain the WhatsApp service. We may share non-personally-identifiable information (such as anonymous user usage data, referring / exit pages and URLs, platform types, asset views, number of clicks, etc.) with interested third-parties to assist them in understanding the usage patterns for certain content, services, advertisements, promotions, and/or functionality on the WhatsApp site.

What can we infer from the above terms of service? To begin with, your contact list becomes public. So if you have saved your colleagues number as Maj ABC, the same is publicly available. You have, therefore, made your colleague's details public without his consent. Additionally, you have to be very careful as to how you enter contact details hereafter. You cannot enter his appointment details in the organisation field as that too becomes public. The public nature of contact details is a matter of concern. In your contact list, you have friends, office contacts and some contacts which you contact infrequently or some contacts which are just there to be contacted on a specified occasion. When you join WhatsApp, all contacts become your 'close' contacts as details get shared. Next, whatever you enter is globally available as the service itself admits that status submissions are globally visible. You need to just look at a few of your friends 'status' to realise how information is being leaked so easily. Cookies are another area of concern. Persistent cookies ensure that

WhatsApp has all the data/information it wants in respect of your browsing history and pattern. It admits to recording your browsing history and nonchalantly states that it shares such information with third party service providers. Visiting armed forces sites like CDA easily give away the information that you are an Army officer.

Use of WhatsApp presents huge risk to privacy and loss of information.

The ease of use of WhatsApp and its popularity comes at a huge risk to your privacy and likelihood of loss of classified information by us or our family members. This service is neither good nor bad; it is ugly from the single point view of massive data loss. This app is best avoided.

To make matters worse, Facebook has bought WhatsApp. So between Facebook and WhatsApp, securing your own privacy has become a bigger challenge. Don't get overwhelmed by it and neither should you give in by thinking that you have no choice. The choice lies in avoiding the services to the maximum extent feasible.

Smartphones

Many officers and soldiers are using Android based smart phones. Given the number of applications accessed on a smartphone everyday, it represents another major source of information leakage. The user is required to give a gmail account when the new phone is loaded with personal and contact data. Most applications have access to contact details, mail details, location data, etc. The user is constantly logged in to various accounts (e-mail, Facebook, Twitter) for ease of use. Thus, the user faces many security threats in the technological field everyday and does not realise its impact on a day to day basis. The downloaded applications, Facebook, WhatsApp, etc have full access to individual data. The user's movements can be geo-located and tracked. The website access can be monitored. Geo-tagged photos carry location data. The images can, thus, give away one's location even though the user may not have mentioned it explicitly anywhere. It is possible to get around some of these issues with little effort. The user can use the smart phones smartly by adhering to a few guidelines.

- Use a gmail account which is not your primary account. If required, create one only for smart phones.
- Never keep logged in to your accounts viz email, Facebook, etc. Though it is inconvenient to log in and log off every time, it is the safer thing to do. At the least, log off from your working email accounts.
- Do not keep your Global Positioning System (GPS) radio button on. Activate it only when you require it to use applications such as Google Maps.

- Carefully read the terms of service of applications you download before using them. Some applications ask for more access than is required. Refrain from downloading such applications.
- Disable geo-tagging while clicking photos.

Should you Delete/Overwrite Data?

What should you do if you posted something you want to delete? Never try to delete anything, always edit and resave the edited data over the old data. All of your information is digital and controlled by a programming code that's always looking for "new" files. These systems are programmed to save all the deleted files, but edited files are backed up onto servers on top of (that is, they overwrite) the old files with the same file name. Old versions of the edited files are kept for a few months (more or less, based on the company policies) but, eventually, the older edited files disappear.

Conclusion

Technology has to function as an enabler, and not create more hindrances for the user. The onus of data security lies with the user. He has to take the requisite steps to secure his data by sensible usage. Also, the easy availability and low cost of smartphones implies that a large number of soldiers today own and operate high end technology. It is also extremely vital to guide and educate our jawans at various functional levels in the nuances of correct usage of various applications as also make them aware of the implications of data loss. It is our collective responsibility to ensure that that both we and our family members follow the guidelines in full earnest to avoid the hazards of social networking and be compliant of the Army Cyber Security Policy.

Col **TS Bains** is a Senior Fellow at CLAWS. Views expressed are personal.

References

http://socialfixer.com/blog/2013/07/29/prevent-facebook-identify-theft-hide-your-friends-list/
http://www.ehow.com/info_8605035_can-keep-identity-hidden-facebook.html
http://www.infoworld.com/article/2617062/internet-privacy/7-ways-to-mask-your-internet-identity.html
http://www.drawbacksof.com/disadvantages-whatsapp/
http://www.ashrafulayan.com/2012/11/whatsapp-addictive-dangerous-read-how.html
http://www.whatsapp.com/legal/
https://securityinabox.org/