"Use your common sense, don't be an idiot": Social Media Security Attitudes amongst Partners of Australian Defence Force Personnel

Amy Johnson, Celeste Lawson and Kate Ames

Partners of serving Australian Defence Force (ADF) members use social media platforms for sharing information and building communities. As privileged insiders, the interactions of partners on Facebook create unique security concerns. This paper examines partner attitudes towards social media security. This paper demonstrates that partners consider themselves security conscious, taking their role in protecting the member and the mission seriously. In the absence of direct advice from the ADF, partners receive information about social media security from peers and civilian sources. This paper offers suggestions which will increase the effectiveness of social media security education for partners.

Partners of Australian Defence Force (ADF) members have increasingly been turning to social media platforms, such as Facebook, for information and support. These groups offer the opportunity to connect with other partners in similar situations, exchange information, make friends and receive support. However, the interactions of ADF partners on Facebook present unique security concerns. This paper discusses the attitudes and behaviours of ADF partners towards social media security, as found in a recent study. International military organisations, including the US military, have attempted to offset the risks arising from the use of social media by developing appropriate policies directly aimed at military families, offering suggestions to keep both the member and their family safe. As yet, the ADF has no such policies or consistent messaging to families about online security. This paper investigates sources of social media education and found in the absence of official advice, the predominant source of information is other ADF partners and concepts of common sense.

ADF partners take social media security seriously, and this research demonstrates how they already consider themselves security aware. They indicated awareness of instances where ADF members do not display appropriate levels of social media security. In addition, partners are confused by the increasingly visible social media presence of the ADF. Partners are resistant to suggestions that further instruction is needed and participants indicated they would not accept restrictions on their social media activity. Importantly, partners want to avoid actions that compromise the safety of the ADF member and their mission. In closing, this paper offers recommendations to the ADF for how it can better engage ADF family

networks on cyber and operational security, with a particular focus on social media.

Background

The use of social media provides numerous benefits to military families, including social support and information gathering. However, there are concerns related to cyber, operational and personal security which must be taken into consideration by the ADF.[119] As one US military family support network stated, "Today's military families and spouses are kept far more informed about troop movements, unit locations, unit activities and more than in years past, but have less training on how to maintain Operational Security".[120] Private Facebook groups, created to facilitate discussion between ADF partners, as well as individual social media pages more broadly, are forums where potentially sensitive information is shared. It can relate to operational security (OPSEC), such as information about deployment locations and dates, or personal security (PERSEC), such as the sharing of home addresses. In addition, frequent changes to privacy settings by social media platforms make it difficult for users to maintain control of their online content.[121]

The ADF currently has no resources specifically targeted to families regarding safe social media use. One isolated article written for Defence families mentioned the importance of maintaining OPSEC and PERSEC but lacked detail on specific measures families can follow to maintain security.[122] The approach taken by the ADF appears to focus on training the serving member in social media safety and then placing the onus on the member to share this information with his or her family. This is a complex issue for the ADF, where its members are required to submit to Defence policy regarding media interaction, but their family members are not, and yet have an

[119] JA. Cigrang, G. Wayne Talcott, J. Tatum, M. Baker, D. Cassidy, S. Sonnek, DK, Snyder, C. Balderrama-Durbin, RE. Heyman and AM. Smith Slep, 'Intimate Partner Communication From the War Zone: A Prospective Study of Relationship Functioning, Communication Frequency, and Combat Effectiveness', *Journal of Marital & Family Therapy*, vol. 40, no. 3 (2014), pp. 332-343; B. Karney and J. Crown, *'Families Under Stress: An assessment of Data, Theory and Research on Marriage and Divorce in the Military*, (2007) RAND Corporation, California, < www.rand.org/content/dam/pubs/monographs/2007/RAND_MG599.pdf >; P. Matthews-Juarez, P.D Juarez and RT. Faulkner, 'Social Media and Military Families: A Perspective', *Journal of Human Behavior in the Social Environment*, vol. 23, no. 6 (2013), pp. 769-776; KR. Rossetto, 'Relational Coping During Deployment: Managing Communication and Connection in Relationships', *Personal Relationships*, vol. 20, no. 3 (2013), pp. 568-586.

[120] BlueStar Families, 'Social Media Guide for Military Families', 2011, < http://www.jber.jb.mil/Portals/144/socialmedia/PDF/socialmedia-Social-Media-Guide-for-Military-Families.pdf > [Accessed 8 September 2015].

[121] D. Brake, *Sharing Our Lives Online: Risks and Exposure in Social Media* (New York: Palgrave MacMillan, 2014).

[122] Defence Family Matters, 'Don't be a twit when you tweet- use social media with care', *Defence Family Matters*, December 2013, p. 14.

increasing array of platforms in which to share their views.[123] Patterson, as the author of a review into the ADF's social media presence, highlighted the need for resources targeted to families.[124] Patterson also considered the US example, and illustrated how the US Department of Defense, using a concept of values-based education which may be successful in an Australian context, engages military families by using "pride and security as primary drivers to inspire families to follow the values and guidelines of OPSEC, rather than a strict set of rules, which would require significant resources to monitor, and be challenging to enforce".[125]

The US Department of Defense, as well as associated military support networks, have created a wide variety of social media support and information resources.[126] These resources overwhelmingly support the military family, including the enlisted member, to be active and engaged on social media networks. They provide practical and specific advice in regards to maintaining OPSEC and PERSEC. This includes cautioning against sharing important dates and explaining modern technology, such as geotagging, which may unknowingly share sensitive information. This contrasts with the experience of military families in Australia where, despite changes to social media policy which are more accepting of members interacting online, a sentiment of being vigilant remains. Concerns over the security of social media data have resulted in claims that ADF members and their families should not maintain any social media presence,[127] however, as normalisation of social media use increases, the practicality of restricting members and families appears unfeasible.

There are currently a large number of private Facebook groups populated by ADF partners. 'Groups' are a popular feature on the social networking platform which facilitate discussion between users based on their shared interests.[128] ADF partner groups are commonly created and managed by partners, who carefully screen new members to confirm their association

[123] Kate Ames, ''Citizen Journalism', the Military and the Media', *Australian Defence Force Journal*, no. 193 (2014), pp. 20-25.
[124] G. Patterson, *Review of Social Media and Defence*, Department of Defence, Australia (2011).
[125] Ibid., p. 87
[126] M. Sherman, M. Kuhl, L. Westerhof, A. Majerle, O. Cheatum, B. Smith, K. Hawkey, J. Rudi, D. Steinham and L. Borden, *Social Media Communication with Military Spouses*, report submitted to US Department of Defense, 2015, < www.reachmilitaryfamilies.umn.edu/sites/default/files/rdoc/Social%20Media%20Communication%20with%20Military%20Spouses.pdf >
[127] M. Mannheim, ''Public Servants should get off social media': warning after Islamic State hack, *The Sydney Morning Herald*, 14 August 2015, online.
[128] N. Park, KF. Kee and S Valenzuela, 'Being Immersed in Social Networking Environment: Facebook Groups, Uses and Gratifications', *CyberPsychology, Behavior and Social Networking,* vol. 12, no. 6 (2009).

with the ADF community. While some groups have a particular topic focus, such as partner employment or housing, others are more general.

Method

Participants in the aforementioned research study were partners of currently serving or recently discharged ADF members. Individual, semi-structured interviews and focus groups collected the insights of thirty-five partners across Australia. Participants were asked to share their opinions of security on social media and also to respond to comments made in the media in relation to ADF members and their families not being permitted to have social media profiles during the member's time of service.[129] Participants primarily related their comments to the social media platform Facebook, and included interactions in private groups as well as their use of the site more generally, such as private messaging. This supports previous studies which indicated that ADF partners predominantly use Facebook for interacting with others in the Defence community.[130] The results presented in this paper form part of the lead author's PhD thesis, which investigates social media use by ADF partners.

Sources of Security Information

> I don't think I've ever seen a communication from Defence about social media.[131]

Currently, ADF members are provided with security briefings about social media as part of their annual mandatory awareness training. In an assessment of this training, the report by Patterson suggested there is a "lack of training and an overt reliance on terms such as 'common sense'".[132] Patterson suggests this leads to misunderstandings on how members should interact online. The expectation appears to be that following this training the ADF member will then communicate what they have learnt to their partners and family members. Despite the importance of families maintaining OPSEC and PERSEC, there are no consistent messages from the ADF directly to partners. Participants in this study indicated they had not received any information from Defence regarding social media security, though in some locations, participants reported social media advice and training is provided to units families at family days and pre-deployment briefings. These briefings are unit specific, and participants who have previously attended a briefing noted finding them generally helpful.

---

[129] M. Mannheim, ''Public Servants should get off social media': warning after Islamic State hack', online.

[130] Atkins, S 2009, A Picture of Australian Defence Force Families 2009: Results from the first survey of Australian Defence Force families, no. DSPPR Report 31/2009, viewed 29 July 2015, http://www.defence.gov.au/dco/documents/ADF_Families_Survey_2009_General_Report.pdf.

[131] Interview with Army partner, age undisclosed.

[132] G. Patterson, *Review of Social Media and Defence*.

Despite this, there is no regular program of pre- or post-deployment briefings across the ADF, with a more substantial number of participants reporting they had never attended, or been given the opportunity to attend, such an event.

Participants revealed that the communication pathway from individual members to their partners is often fractured. Participants in focus groups stated their partner did not reliably pass on messages from the unit, even when those messages directly impacted the partner, such as community meetings and Defence Community Organisation (DCO) events. Few participants said their partners were good communicators, and only one participant said she talked directly with her partner about social media behaviour.

> We kind of talk about it. He's told me what's appropriate and what's not because he's done the media course in the Defence. So we know what to do.[133]

This suggests the current model of social media education for partners, which is delivered via the member, is ineffective. Consequently, because partners are not receiving messages about social media security from either the ADF or the member, partners seek out advice from other sources. Participants reported receiving information about social media security from their workplace and from friends. Participants also made their own assumptions, including adopting social media policies written for ADF members, as well as using 'common sense' when figuring out what to do.

> If defence is sending out a memo asking the media to be respectful to OPSEC, naturally that applies to all of us as well.[134]

> You know, use your common sense, don't be an idiot. Pretty much. We know what we can and can't write. We are lucky to be in a position where we could write something that we probably shouldn't have.[135]

Participants in both interviews and focus groups identified ADF partner Facebook groups as a source of information on social media security.

> Most of the information I get about what you can and can't post on social media, I get from the Defence wives Facebook pages.[136]

In the absence of official advice, the ADF partner Facebook groups are self-moderating, although the administrators of groups said they considered it their responsibility to maintain OPSEC, and discussed sending out messages to partners who put sensitive information on group pages.

---

[133] Interview with Navy partner, aged 34.

[134] Interview with Army partner, age undisclosed.

[135] Interview with Army partner, aged 38.

[136] Interview with Army partner, aged 23.

> We will delete and then send them a message saying OPSEC. I understand you can do whatever you like [in some groups], but in our group, it's not allowed.[137]

Security Awareness and Social Media Training

ADF partners take online security seriously. Participants discussed being careful with what they post online, and they consider themselves to be 'security aware'. Participants were aware they couldn't share specific homecoming dates and felt confident their profiles were restricted, giving them control of their content.

> I'm quite careful with what groups I go into and what I put up there. I'm notorious for deleting old Facebook posts and old posts and things. So I do keep my privacy quite restricted, and I will go through periodically every now and then and delete old stuff.[138]

> A lot of us went through our pages and checked and made sure it was locked down. And most of us aren't so stupid that we overtly say, "My husband is in Afghanistan at (location) compound", we say, "My husband has been deployed".[139]

One participant explained how she used a combination of common sense and prior knowledge to ensure her activities on social media did not cause security concerns.

> So we are fairly savvy, I'm not the one who sits at home and says "Oh, my husband is going away for six months, Oh when does he leave? Oh, he leaves on the sixteenth of January on this flight? Oh, where is he going? Oh, he's going here?". No, that's not me. I'm smarter than that. I've been schooled in the way of how things work.[140]

While participants spoke positively about the prospect of social media training delivered by ADF representatives, the detailed analysis of comments revealed partner attitudes relating to social media security would influence the successful implantation of social media training. Participants contended they were confident social media users who successfully manage their online activity in consideration of OPSEC principles. Participants who were active online were supportive of the concept of training, but typically indicated they would not attend themselves, believing they have a sufficient understanding of social media security. This understanding appears to be built from a combination of information from various unofficial sources, as well as common sense. This was demonstrated directly by the comments of one interview participant who identified she did not feel she had any need for instruction but understands other partners might.

---

[137] Interview with Army partner, aged 38.

[138] Interview with Navy partner, aged 34.

[139] Interview with Air Force partner, aged 42.

[140] Interview with Air Force partner, aged 42.

> I think it would probably be good. Like personally, I don't have any issues, I just use common sense, but some people don't seem to have (common sense).[141]

Social Media Restrictions for Partners

Participants were asked to comment on whether they would be receptive to requests from the ADF to close their social media profiles. This question was prompted by a media article which claimed that public servants, including ADF members, should not have active social media profiles during service.[142] Participants were resistant to closing their social media profiles, though most could see why the ADF may be encouraged to instigate restrictions. The only participant who agreed that social media restrictions were necessary was in a dual-serving relationship and had already deleted her Facebook profile, citing security and privacy concerns.

Participants gave several reasons for their resistance to accepting social media restrictions from the ADF. The first of these reasons was that participants considered restrictions to be unrealistic. They explained how social media was an intrinsic part of life, and the practicality of policing restrictions would be incredibly difficult. Participants also questioned the authority of the ADF to make a request like this of civilian partners.

> I can't see them being able to enforce that if they did it. I can't see how they are going to enforce it; it sounds like a crazy thing even to attempt. I can see why they'd want to do it, but that would just make people make up an alias, and they'd just be online but under an alias rather than their real names, and that would just cause more issues.[143]

> You are going to keep stripping them of normal life, once again. You are going just to keep creating conflicts. What we actually need to do is recognise that there are certain aspects of society we can't control, like social media.[144]

Another reason participants identified that restrictions on social media for ADF partners would not be advisable was because it would isolate partners further, and place unfair restrictions on partners who use social media for employment. One participant spoke passionately about how social media gave her a valued social and community outlet while she was caring for her young family, away from support networks.

---

[141] Interview with Navy partner, aged 34.

[142] M. Mannheim, ''Public Servants should get off social media': warning after Islamic State hack', online.

[143] Interview with Air Force partner, aged 42.

[144] Interview with ex-Navy partner, aged 30.

> I'd end up killing my children and myself. It's my only form of contact with the outside world that is not my little bubble of … children and baby. They could charge my husband before they could get rid of my Facebook.[145]

In addition to facilitating connections with friends, family and networks, participants discussed finding social media useful for communicating with their partner, especially during deployments. Several discussed how the member was previously absent from social media but created Facebook profiles during deployments so they could interact with their family at home. Issues surrounding access to email-enabled computers and restrictions of email file sizes were also reasons that partners would communicate with the member using social media rather than email.

> It was my daughter's birthday last week, so I tried to send a photo via e-mail, and it came back because the file was too big for one photo … Whereas with Facebook I can send hundreds, tag him in things, and he's a bit the same, "Yeah, we just pulled in, and I've got Wi-Fi, how are you going?". It is awesome just to know that.[146]

Protecting the Member and the Mission

Despite partners considering that they were already sufficient at managing social media security, a consistent theme was their concern for the safety and well-being of the member. Participants expressed their concern that their actions, or the actions of others, could have a negative impact on the mission, or compromise safety. This was the only situation in which the participants were receptive to changing their social media habits.

> I don't want to be the reason that anyone else gets hurt. I don't want to post a picture and be the reason that, really dramatic, someone gets bombed. I don't want to be the reason for that, so that's why I won't do it. Not because Defence told me to.[147]

> I sure would be [expletive deleted] if something happened to my partner because someone else's partner from the same ship decided to go, 'Oh my god, they are coming home at this time in three days', and the ship gets delayed because you just ruined the whole (thing). There's an unlikely chance that will happen, but I don't want to run that risk.[148]

Confusion about the ADF's Activity on Social Media

Overwhelmingly, participants spoke positively of Defence's recent increased activity on social media networks. Participants said they enjoyed being able to see parts of their partner's life they might not usually. Participants with children enjoyed being able to show them the posts and used these images to strengthen the relationship between member and dependants.

---

145 Interview with Army partner, aged 29

146 Interview with Navy partner, aged 31+.

147 Interview with Army partner, aged 33.

148 Interview with Navy partner, aged 27.

> It's really good, and the kids love seeing him do stuff, in vehicles, holding weapons, whatever, the kids love seeing him, so I love that they do that here.[149]

> You know, seeing photos of the boats sometimes, if you can't talk to them or whatever, you can see a picture on there and think, Oh, you're on there, you're alive.[150]

Despite enjoying reading the posts, participants reported feeling confused about privacy and security implications. The interactions of Defence on social media, including photos of members in uniform, is in contrast to the actions they perceive as restricted on social media networks.

> It would be interesting to explore a little bit the inconsistencies with the Australian Army posts, like …they've posted (photos) in uniform, fighting, names. It's very inconsistent with the expectations.[151]

> But then what's the line? If they are allowed to post it, are we?[152]

Participants commented on how the members themselves were not always security aware, despite being the ones who receive the training. Participants in one focus group referenced Exercise Hamel, where the planned training event was reportedly compromised by soldiers posting content on social media networks that enabled opposing forces to ascertain the location of deployed forces.[153]

> People post photos, and they are all geotagged, so then the other party can find them, which is what happened at Exercise Hamel. They were all posting photos, they were all geotagged, so their opposition found them.[154]

In other focus groups and interviews, participants shared examples of times when members had contravened OPSEC principles online. A number of participants said they managed the members' social media profiles, which included changing security settings, adding or removing content, and editing personal information such as display names. These participants felt they were more aware of the risks resulting from activity on social media, both from a security and a reputational perspective, than their partner, and they took an active role in managing this risk for the member.

---

[149] Interview with Army partner, aged 33.

[150] Interview with Navy partner, aged 31+.

[151] Interview with Navy partner, aged 33.

[152] Interview with Army partner, aged 23.

[153] M.Ryan and M. Thompson, 'Social Media in the Military: Opportunities, Perils and a Safe Middle Path', < www.groundedcuriosity.com/social-media/in-the-military-opportunities-perils-and-a-safe-middle-path > [Accessed 31 August 2017].

[154] Interview with Army partner, aged 40.

Discussion and Recommendations

Partners would likely benefit from specific training, particularly as this study indicates partners can take an active role in managing the ADF member's social media profiles. Partners being excluded from conversations regarding the current online environment may encourage false feelings of confidence in their ability to maintain online security. Despite the value of providing social media security information, the ADF faces challenges in successfully delivering this training to partners. Participants in this study were supportive of social media training; however, their support is given on the expectation that others would benefit, as most do not perceive a personal need to receive advice or instruction.

A key finding of this research is that it would be futile to place restrictions on the social media activity of ADF partners. In addition to making comments that highlighted restrictions would be challenging to enforce, participants were forthcoming in stating they were not enlisted military members, and as such did not need to comply with instructions from the ADF. Indeed, efforts to educate partners about social media could be perceived as 'control', and negatively impact on the relationship between partners and the ADF.

In planning and delivering social media training to partners, a more effective approach would be to align the training with partners' strong sense of willingness to avoid danger to the member. Training focused around 'Keeping your Defence member safe' would align with the values that ADF partners hold. Successful advice and training would also be that which acknowledges the partners' separate, civilian identity, and offers to improve their existing social media security knowledge. This value-based education fits with the model of partner education and training offered to US military families, where "educational material focuses on instilling pride in the family members by letting them know they are as much a part of the military community as their soldier, with their own responsibilities for keeping the soldier safe".[155]

One of the most significant challenges would be disseminating the message to partners. The Patterson report suggested that the Defence Community Organisation and associated support organisations could be responsible for distributing training and information to partners; however, participants in this research identified breakdowns in communication between those organisations and partners. For this reason, organisations like DCO may not be well positioned to deliver this training to partners. Participants who attended pre-deployment briefings found them valuable, so the extension of these briefings to more units across the ADF would appear to be beneficial. The placement of engaging and relevant social media security advice at these events would be key. In addition, information which can be easily

[155] G. Patterson, *Review of Social Media and Defence,* p. 87.

shared on social media networks by ADF partners, who already do the majority of self-education regarding online security, would take advantage of these already strong pathways. For instance, social media graphics which give instruction on how to interact online may be well received by partners. Partners who are active in their communities could share these graphics, which encourages others to engage in better practice.

Future research which compares social media security attitudes against actual social media activity may reveal differences between partners' perception of their own social media awareness, and actual content they post online. Such research could be used to build education programs. Research comparing perceptions of behaviour would also overcome the bias present in self-reported data. In addition, investigations of ADF interactions on social platforms other than Facebook, such as SnapChat or Twitter, would increase depths of understanding on this issue.

Conclusion

This paper has presented a discussion about social media security in relation to the activities of ADF partners online. It notes that partners do not currently receive consistent instruction or advice about social media from the ADF. The current method of social media training is an expectation that members will discuss issues of security with their partners, although this is not always happening. Partners who were able to attend pre-deployment or similar briefings where social media instruction was given found these briefings helpful. In the absence of social media instruction from Defence or members, ADF partners are receiving social media advice primarily from other ADF partners, as well as incorporating aspects of training received from civilian workplaces and other sources. This paper also found that partners perceive ADF members as not being particularly security conscious, and some participants managed the members' social media profile on their behalf.

Participants generally considered themselves security aware and generally in control of the content they place online. Many participants reported that social media safety was primarily about 'common sense', and suggested that the majority of operational security issues on social media happened to people of specific demographic groups, such as younger partners. Despite this, partners reported being receptive to social media training from the ADF, with one participant reporting that training should be compulsory for partners. A significant finding in this paper is that owing to the strength of conviction in their own security awareness, partners would not attend training if it was offered.

Participants were aware of the negative implications of posting sensitive information about the military online, and they wanted to avoid behaviour that would place their partner or the broader ADF in danger. Participants

also reported feeling confused about the ADF's activities on social media and highlighted differences between what the ADF posts online, and what partners perceive they are and are not allowed to post. Participants also gave examples of ADF members posting inappropriate content on social media.

In closing, this paper identified the challenges faced by those tasked to provide training and education on social media security to partners. It has argued the restriction of partners on social media networks is futile, due to the partner's separate identity and sense of autonomy. It has also offered a series of suggestions, firstly to align training and education to the partner's keen sense of danger avoidance. Participants in this research strongly contended they did not want their actions on social media to be responsible for placing their partner, or the broader mission, in jeopardy. Training that aligns with this value will be effective. This paper also suggested pre-deployment briefings, which currently only take place on a limited number of unit deployments, could be supported across the wider ADF, and social media training could take place at these briefings. Finally, this paper suggested that given the evidence the majority of information regarding social media security is generated by and shared amongst ADF partners themselves, education from the ADF would be beneficial in a format that can be disseminated via social media platforms. This would take advantage of already strong ADF partner networks.

Social media security is an important issue, and there is cause for concern regarding the social media interactions of ADF partners. This study reported in this paper provides a unique view in that it identified the sources where partners received information and training, and the challenges associated with the ADF providing training on social media.

Amy Johnson is a CQUniversity PhD candidate and Casual Academic. Her PhD investigates social media use by Australian Defence Force partners. This research was supported by the Australian Government Research Training Program (RTP). Amy is interested in social media, the military and sociology. a.johnson2@cqu.edu.au.

Associate Professor Celeste Lawson is the Head of CQUniversity's Professional Communication degree. She has extensive practical experience in journalism and policing. She currently researches in social media, communication and public relations, with a focus on pedagogy and learning. Celeste teaches undergraduate and postgraduate students in public relations and communication. c.lawson@cqu.edu.au

Associate Professor Kate Ames is a cultural sociologist whose scholarship is in the area of culture, language, and interaction. She has a background in journalism and public relations which are her areas of teaching. Kate is also a military public affairs officer with the Australian Army (Reserve) and is currently posted in an instructional role. k.ames@cqu.edu.au